

# CARMICHAEL NUMBER VARIABLE RELATIONS: THREE-PRIME CARMICHAEL NUMBERS UP TO $10^{24}$

J.M.CHICK

ABSTRACT. Bounds and other relations involving variables connected with Carmichael numbers are reviewed and extended. Families of numbers or individual numbers attaining or approaching these bounds are given. A new algorithm for finding three-prime Carmichael numbers is described, with its implementation up to  $10^{24}$ . Statistics relevant to the distribution of three-prime Carmichael numbers are given, with particular reference to the conjecture of Granville and Pomerance in [10].

## 1. INTRODUCTION

A Carmichael number  $n$  is defined by the property that  $n$  is composite and  $a^n \equiv a \pmod{n}$  for all  $a$ . For  $n = \prod_{i=1}^d p_i^{\alpha_i}$ , with  $p_i$  prime, Korselt in 1899 [11] stated that  $\alpha_i = 1$  for all  $i$  and  $\text{lcm}(p_1 - 1, p_2 - 1, \dots, p_d - 1)$  divides  $(n - 1)$  is a necessary and sufficient condition for  $n$  to divide  $(a^n - a)$ , but he did not exhibit any such number  $n$ . In 1910 Carmichael [3] showed that the above condition required  $d \geq 3$  and all  $p_i$  to be odd, and gave four such numbers, the smallest of which was  $561 = 3 \cdot 11 \cdot 17$ . In 1912 [4] he amplified his remarks and extended his list to fifteen such numbers, including one with  $d = 4$  (although very curiously he reconsidered and rejected 561!)

Korselt's criterion, stated above, is the basis for much of the theory on Carmichael numbers and for algorithms to find them, including ours. For a background on Carmichael numbers and previous counts of Carmichaels up to increasing upper bounds see Ribenboim [16], counts which have now culminated in Richard Pinch's up to  $10^{18}$  [13]. Our list up to  $10^{24}$  for  $d = 3$  may be found on the website of the Cambridge University Department of Pure Mathematics and Mathematical Statistics [7].

In addition to  $p_i$  and  $n$  already mentioned, Korselt's criterion spawns numerous other variables, some of them specific to  $d = 3$ , and various relationships and bounds connecting them are of value in constructing algorithms to find Carmichael numbers as well as being of interest in themselves. In the next three sections we review and extend such relationships and bounds.

## 2. NOTATION; VARIABLES; KORSELT FACTORISATIONS, NUMBERS AND FAMILIES

**2.1. Notation, KN's and K-families.** Because of the form of the Korselt criterion, we shall find it convenient consistently and exclusively to use the abbreviation  $x' := x - 1$ . So we have  $(xy)' = xy' + x' = x'y' + x' + y'$ , etc. We shall also consistently use the notation which we define during §2, without repeated explanation.

---

2000 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11Y55.

*Key words and phrases.* Carmichael numbers.

Let  $n = \prod_{i=1}^d p_i$ , where  $1 < p_1 < p_2 < \dots < p_d$  and  $d \geq 3$ , be a number for which the factors  $p_i$  satisfy the condition  $p_i'$  divides  $n'$ , and define  $P := \prod_{i=1}^{d-2} p_i$ ,  $p := p_1$ ,  $q := p_{d-1}$  and  $r := p_d$ , so for  $d = 3$ ,  $n = pqr$ . Let  $P_i := n/p_i$ , so  $n = p_i P_i$  for  $1 \leq i \leq d$ , and similarly write  $n = qQ = rR$ .

Then  $n' = (p_i P_i)' = p_i' P_i + P_i'$ , so  $n' \equiv 0 \pmod{p_i'}$  gives  $P_i' \equiv 0 \pmod{p_i'}$  for  $1 \leq i \leq d$ , and conversely.

Thus there exist integers  $\lambda_i$  such that  $P_i' = \lambda_i p_i'$ . Also if  $\lambda_d = 1$ , then obviously  $p_d = P_d = \prod_{i=1}^{d-1} p_i$  is *necessarily* composite (usually we shall assume that  $\lambda_d \geq 2$ ). We write  $D := \lambda_{d-1}$ ,  $E := \lambda_d$ , so

$$(2.1) \quad Q' = Dq' \quad \text{and} \quad R' = Er'$$

So far in substance but not in notation we follow Carmichael, if  $p_i$  are all odd primes. But both for algorithms and theoretical results it is often necessary to consider sets of numbers  $n$  with a factorisation which satisfies the Korselt divisibility criterion without all (or any) of the factors necessarily being prime: such a number,  $n$  as above, together with the particular Korselt factorisation, we shall term a *Korselt number* (abbreviated to  $KN$ , or  $K_d N$  if its Korselt factorisation has  $d$  factors) if, for all  $i$ ,  $p_i$  is odd and  $E \geq 2$ . I have not established whether it is possible for a number to be a  $K_3 N$  in more than one way, but the Korselt factorisation will always be apparent from the context. Clearly if every  $p_i$  is a prime then  $n$  is a Carmichael number, which we shall abbreviate to  $CN$  or  $C_d N$  in like manner. We shall also consider certain families of  $KN$ s ( $K$ -families or  $K_d$ -families) of the type  $n(t) = \prod_{i=1}^d p_i(t)$ , where  $n$  and  $p_i$  are polynomials over the integers and  $t$  is a non-negative integer parameter. It seems plausible to conjecture (with Schinzel, see page 91 of [16]) that any  $K$ -family will contain an infinite number of  $CN$ 's unless, speaking loosely, there is some *obvious* reason why (almost) all members have at least one composite  $p_i$ .

**2.2. Chernick's universal forms.** The best known  $K$ -families are the “universal forms” described by Chernick in 1939 [5], and it will be helpful to summarise his theory in our notation. Let  $n$  be any  $KN$ . Then we have

$$(2.2) \quad n' = \prod_{i=1}^d (p_i' + 1) - 1 = \prod_{i=1}^d p_i' + \sum (p_1' p_2' \cdots p_{d-1}') + \dots + \sum p_1' p_2' + \sum p_1'$$

Let  $H = \gcd_{i \neq j} \{p_i'\}$  for any particular  $j$ . Then from (2.2)  $n' \equiv p_j' \pmod{H}$ . But since  $n$  is a  $KN$ , clearly for  $i \neq j$  we have  $H | p_i' | n'$ , so  $n' \equiv 0 \pmod{H}$ . Hence  $p_j' \equiv 0 \pmod{H}$ , whence  $H = \gcd_{1 \leq i \leq d} \{p_i'\}$ . So if  $A_i := p_i'/H$ , any set of  $(d-1)A_i$ 's are coprime, i.e.

$$(2.3) \quad \gcd_{i \neq j} \{A_i\} = 1, \text{ for } 1 \leq j \leq d$$

Also if  $L := \text{lcm}_{1 \leq i \leq d} \{p_i'\}$  and  $\ell := \text{lcm}_{1 \leq i \leq d} \{A_i\}$ , clearly  $L = \ell H$ . Combining  $p_i' = A_i H$ ,  $L = \ell H$  and  $n' \equiv 0 \pmod{L}$  with (2.2), we get

$$(2.4) \quad \begin{aligned} & H^{d-2} \sum A_1 A_2 \cdots A_{d-1} + H^{d-3} \sum A_1 A_2 \cdots A_{d-2} \\ & + \cdots + H \sum A_1 A_2 + \sum A_1 \equiv 0 \pmod{\ell} \end{aligned}$$

Suppose now that we are given any set  $\{A_1, A_2, \dots, A_d\}$  satisfying (2.3), then congruence (2.4) is always soluble for  $H$  when  $d = 3$  (see below, following (2.5)), but not necessarily when  $d > 3$ . If  $H_o$  is any solution, then so is  $H_t = H_o + t\ell$ , so we can choose  $H_o$  to satisfy  $1 \leq H_o \leq \ell$ . Then if we take  $p_i = A_i H_t + 1 = A_i \ell t + A_i H_o + 1$  and  $n = \prod_{i=1}^d p_i$ ,  $n$  satisfies the Korselt criterion for all  $t$ , and with certain precautions yields a  $K_d$ -family corresponding to each basic solution  $H_o$  (precautions: our definition of a  $KN$  requires (i) all  $p_i$  are odd, and (ii)  $E \geq 2$ : for (i), if  $\ell$  is even and  $H$  is odd, from (2.4) we get

$$\sum (A_1 A_2 \cdots A_{d-1}) + \cdots + \sum A_1 A_2 + \sum A_1 = \prod_{i=1}^d (A_i + 1) - \prod_{i=1}^d A_i - 1 \equiv 0 \pmod{2},$$

whence since  $\ell \mid \prod_{i=1}^d A_i$  and  $\ell$  is even,  $\prod_{i=1}^d (A_i + 1) \equiv 1 \pmod{2}$  and so for all  $i$ ,  $A_i \equiv 0 \pmod{2}$ , contradicting (2.3) which holds by hypothesis; so if  $\ell$  is even then  $H$  is even and all  $p_i$  are odd; but  $\ell$  is odd iff all  $A_i$  are odd, so  $H_t$  is alternately odd or even as  $t$  increases, and then the  $K$ -family will be generated by the parameter  $u$  where  $t = 2u$  or  $2u + 1$  according as  $H_o$  is even or odd; while for (ii),  $E \geq 2$ , it may be necessary to exclude  $t = 0$  from the family). These  $K$ -families are Chernick's universal forms, of which the best known arises from  $(A_1, A_2, A_3) = (1, 2, 3)$  with  $H_o = 6$  and then as above  $n = (6t + 7)(12t + 13)(18t + 19)$  (Chernick equivalently has  $(6M + 1)(12M + 1)(18M + 1)$ ).

For  $d = 3$ , let  $A := A_1$ ,  $B := A_2$ ,  $C := A_3$ . Then, for any  $K_3N$ , from (2.3)  $A$ ,  $B$ ,  $C$  are pairwise coprime,  $\ell = ABC$ , and so from (2.4) there exists a positive integer  $F$  such that

$$(2.5a) \quad H(AB + AC + BC) + A + B + C = FABC, \quad \text{i.e.}$$

$$(2.5b) \quad F = H \left( \frac{1}{A} + \frac{1}{B} + \frac{1}{C} \right) + \frac{1}{AB} + \frac{1}{AC} + \frac{1}{BC} \quad \text{is a positive integer.}$$

Also given any pairwise coprime  $A$ ,  $B$ ,  $C$ , then  $\sum AB$  and  $ABC$  are coprime, so (2.5a) has a unique solution for  $F$  and  $H_o$ , and we get a  $K_3$ -family as described above. Putting  $p_i' = A_i H$  in (2.2) with  $d = 3$ , with (2.5a) we have

$$(2.6) \quad n' = ABCH(H^2 + F)$$

**Theorem 2.1.** *For any  $K_3N$ ,  $1 \leq F \leq 2H$ .*

*Proof.* Based on (2.5b), write  $F = F(A, B, C, H)$ . We have  $H \geq 2$  and  $B \geq 2$ . Obviously  $F \geq 1$ . We consider two cases: (a)  $B \geq 3$ , (b)  $B = 2$ .

$$(a) \text{ For } B \geq 3, F(A, B, C, H) \leq F(1, 3, 4, H) = \frac{19H}{12} + \frac{2}{3} < 2H \text{ for } H \geq 2,$$

$$(b) B=2. \text{ For } C \geq 7 \text{ we have } F(1, 2, C, H) \leq F(1, 2, 7, H) = \frac{23H}{14} + \frac{5}{7} \leq 2H \text{ for } H \geq 2. \text{ Also}$$

$$F(1, 2, 5, H) < F(1, 2, 3, H) = \frac{11H}{6} + 1 \leq 2H \text{ for } H \geq 6.$$

But for  $(A, B, C) = (1, 2, 3)$  or  $(1, 2, 5)$  we have  $H_o = 6$ , whence the result, with  $F = 2H$  only for  $n = 7 \cdot 13 \cdot 19 = 1729$ .  $\square$

Note:  $(A, B, C, H) = (1, 2, 7, 2)$  yields  $n = 3 \cdot 5 \cdot 15 = 225$ , not a  $K_3N$  since  $E = 1$ .

**2.3. The equation(s) of Beeger, Duparc and Pinch.** For any  $KN$  we have  $n = Pqr = qQ = rR$ , and hence  $Q = Pr$  and  $R = Pq$ .

Then from (2.1)  $Dq' = Q' = (Pr)' = Pr' + P'$ , so

$$(2.7) \quad Dq' - Pr' = P', \text{ and similarly } Er' - Pq' = P'.$$

Solving simultaneously for  $q'$  and  $r'$ , and writing

$$(2.8) \quad \Delta := DE - P^2, \quad \text{we get}$$

$$(2.9a) \quad q' = \frac{P'(P+E)}{\Delta} \quad \text{and}$$

$$(2.9b) \quad r' = \frac{P'(P+D)}{\Delta}.$$

Beeger for  $d = 3$  in 1950 [2] and Duparc for  $d \geq 3$  in 1952 [9] gave (2.9a), and Pinch [12] bases his first algorithm on (2.9). From (2.9),  $\Delta \geq 1$ . Also Duparc showed

**Theorem 2.2.** *For any  $KN$ ,  $2 \leq E \leq P - 1$ .*

*Proof.* From the definition of a  $KN$ ,  $E \geq 2$ . Also  $r - q - 1 \geq 1$ . Hence from (2.7)

$$E = \frac{Pq' + P'}{r'} = \frac{Pr' - P(r' - q') + P'}{r'} = P - \frac{P(r - q - 1) + 1}{r'} < P,$$

whence the result.  $\square$

The following equations based on (2.8) and (2.9) will also be useful in §3 and §4. Define  $s := P - E$  and  $\eta := D - P - s$ , so

$$(2.10) \quad E = P - s \text{ and } D = P + s + \eta$$

Then from Theorem 2.2,  $1 \leq s \leq P - 2$ , and from (2.8) we have

$$(2.11) \quad \Delta = \eta(P - s) - s^2, \text{ whence } \eta = \frac{\Delta + s^2}{P - s} = \frac{\Delta + s^2}{E} \text{ and so } \eta \geq 1$$

Hence

$$(2.12) \quad s^2 + \eta s = \eta P - \Delta, \quad \text{so } \Delta < \eta P, \quad \text{and } s = \sqrt{\eta P - \Delta + \frac{\eta^2}{4}} - \frac{\eta}{2}$$

Hence if

$$(2.13a) \quad \theta := \sqrt{4(\eta P - \Delta) + \eta^2}, \quad \text{then}$$

$$(2.13b) \quad s = \frac{\theta - \eta}{2}, \quad E = P - \frac{\theta - \eta}{2}, \quad D = P + \frac{\theta + \eta}{2}$$

Then (2.9) becomes

$$(2.14a) \quad q = \frac{P'}{\Delta} \left( 2P + \frac{\eta - \theta}{2} \right) + 1,$$

$$(2.14b) \quad r = \frac{P'}{\Delta} \left( 2P + \frac{\eta + \theta}{2} \right) + 1,$$

$$\text{whence } qr = \frac{P'^2}{\Delta^2} \left\{ \left( 2P + \frac{\eta}{2} \right)^2 - \frac{\theta^2}{4} \right\} + \frac{P'}{\Delta} (4P + \eta) + 1$$

and using (2.13a) for  $\theta^2$  we get

$$(2.15) \quad n = Pqr = P \left\{ \frac{P'^2}{\Delta^2} (4P^2 + \eta P + \Delta) + \frac{P'}{\Delta} (4P + \eta) + 1 \right\}$$

Subject to the solubility of certain congruences, a particular choice of  $\Delta$  and  $\eta$  leads to one or more  $K_3$ -families via (2.12, 2.13, 2.14), using (2.12) with  $s$  as a first parameter.

**2.4. Relations connecting  $K_3N$  variables.** These will be needed in §4.

$$\text{We have } E = \frac{R'}{r'} = \frac{(pq)'}{r'} = \frac{p'q' + p' + q'}{r'} = \frac{ABH + A + B}{C},$$

since  $p_i' = A_iH$ , and hence

$$(2.16) \quad C = \frac{ABH + A + B}{E} = \frac{Bp + A}{E}.$$

Combining this with (2.5a) we get  $ABCF = CE + CH(A + B) + C$ , i.e.

$$(2.17) \quad ABF = (A + B)H + E + 1, \quad \text{whence, writing}$$

$$(2.18) \quad G := AF - H, \quad \text{we have}$$

$$(2.19) \quad B = \frac{AH + E + 1}{G} = \frac{p + E}{G}.$$

$$\text{Also using (2.9a), } BH = q' = \frac{p'(p + E)}{\Delta} = \frac{AH(p + E)}{\Delta}, \text{ so } B = \frac{A(p + E)}{\Delta},$$

whence from (2.19),

$$(2.20) \quad \Delta = AG.$$

So  $G \geq 1$ , we have  $\Delta \geq 1$ , and we now show

**Theorem 2.3.** *For any  $K_3N$ ,  $1 \leq G < 2H$  and  $1 \leq \Delta < 2p - 2$ .*

*Proof.* We have  $p < q'$  and, from Theorem 2.2,  $E \leq p'$ . Hence, using (2.20) and (2.9a),

$$AG = \Delta = \frac{p'(p + E)}{q'} < \frac{p'(2p - 1)}{p} = 2p - 3 + \frac{1}{p} = 2AH - 1 + \frac{1}{p} < 2AH = 2p',$$

from which both statements in Theorem 2.3 follow.  $\square$

We observe that (2.18, 2.19, 2.16) enable us to express in turn  $A$ ,  $p$ ,  $B$ ,  $q$ ,  $C$ ,  $r$  and  $n$  in terms of  $E$ ,  $F$ ,  $G$  and  $H$ , which we shall exploit later.

**2.5. Bounds, variables and challenges.** The next two sections are concerned with finding inequalities  $y \leq f(x)$  showing upper bounds for  $y$  given  $x$ , where  $x$  and  $y$  are variables connected with  $KN$ 's and hence  $CN$ 's. Here  $f$  is an increasing function and, usually,  $x$  is  $P$ ,  $p$  or  $n$ : for example, we shall show that an upper bound for  $r$  given  $n$  is given by  $r \leq \lceil \sqrt{\frac{n}{2}} \rceil$ . Obviously, if  $f^{-1}$  exists, any such relation is equivalent to a lower bound of  $f^{-1}(y)$  for  $x$  given  $y$ . Also, if  $x$  is  $n$  and we are looking for all  $CN$ 's less than some large  $X$ , we have  $y \leq f(X)$ . Our symbols have been defined as integer variables connected with  $KN$ 's, but sometimes we shall treat them as real variables obeying the same inequalities as the integer variables. If possible we shall exhibit  $K$ -families for which the bound is attained, or failing that some  $CN$ 's or  $KN$ 's for which it is approached. Some of these bounds were used in executing our algorithm for  $C_3N$ 's (see §5), although invariably a weaker (and more easily proved) bound would have sufficed.

Challenges: occasionally I offer a challenge to find a  $C_3N$  or  $K_3N$  satisfying certain conditions, and I would be very interested to receive successful responses at my address at the end of this paper.

### 3. BOUNDS FOR $KN$ VARIABLES WITH $d \geq 3$

#### 3.1. Upper bounds given $P$ for $q$ , $r$ and $n$ .

**Theorem 3.1.** (*Duparc's theorem*) For any  $KN$ ,

$$q \leq (P-1) \left( 2P + \frac{1}{2} - \sqrt{P - \frac{3}{4}} \right) + 1 .$$

*Proof.* From (2.9a) and Theorem 2.2, if  $\Delta \geq 2$  we have

$$(3.1) \quad q' = \frac{P'(P+E)}{\Delta} \leq \frac{P'(P+P')}{2} = P' \left( P - \frac{1}{2} \right)$$

Fix  $\Delta$  and  $P$ , with  $\Delta < P$ , and regard  $\theta = \theta(\eta)$  and  $q = q(\eta)$  as functions of a real variable  $\eta$ , defined by (2.13a) and (2.14a) respectively, with  $\eta = \eta_o$  for the  $KN$  under consideration. Then we have

$$(3.2) \quad \frac{d}{d\eta}(\eta - \theta) = 1 - \frac{\eta + 2P}{\sqrt{(\eta + 2P)^2 - 4(P^2 + \Delta)}} < 0 ,$$

so as  $\eta$  increases,  $\eta - \theta$  and hence  $q$  both decrease, and hence  $q(\eta_o) \leq q(1)$ . We shall use (3.2) for general  $\Delta$  later, but with  $\Delta = 1$ ,  $q(1) = P'(2P + \frac{1}{2} - \sqrt{P - \frac{3}{4}}) + 1$ . But for  $P \geq 3$ ,  $P'(P - \frac{1}{2}) < P'(2P + \frac{1}{2} - \sqrt{P - \frac{3}{4}})$ , so with (3.1) the result follows.  $\square$

We note that for this maximal  $q$  situation, with  $\Delta = \eta = 1$ , (2.15) gives

$$(3.3) \quad n = N_2(P) := 4P^5 - 7P^4 + 7P^3 - 4P^2 + P$$

Also from (2.12, 2.13, 2.14) we get

$$(3.4)$$

$$P = p_2(s) := s^2 + s + 1 , \quad \theta = 2s + 1$$

$$q = Q_2(P) := (P-1) \left( 2P + \frac{1}{2} - \sqrt{P - \frac{3}{4}} \right) + 1 = q_2(s) := 2s^4 + 3s^3 + 3s^2 + 2s + 1$$

$$r = R_2(P) := (P-1) \left( 2P + \frac{1}{2} + \sqrt{P - \frac{3}{4}} \right) + 1 = r_2(s) := 2s^4 + 5s^3 + 6s^2 + 3s + 1$$

and we have the  $q$ -maximal  $K_3$ -family  $n = n_2(s) := p_2(s) \cdot q_2(s) \cdot r_2(s)$ . A computer search by Ian Williams (see §7) for  $1 \leq s \leq 4906$  found just 12  $q$ -maximal  $C_3N$ 's, with  $s = 1, 2, 6, 90, \dots$  up to 3654, and only one  $q$ -maximal  $C_dN$  with  $d > 3$ , namely the  $C_6N$   $n_2(1493) = 7 \cdot 19 \cdot 31 \cdot 541 \cdot 9947309489407 \cdot 9953972118361 \simeq 2.2 \times 10^{32}$ , with  $P = 2230543$ .

**Theorem 3.2.** *For any  $KN$ ,  $r \leq R_3(P) := \frac{1}{2}(P-1)(P+1)^2 + 1$ , with equality iff  $q = Q_3(P) := P^2 + P - 1$ .*

*Proof.* From (2.8) and (2.9b),

$$r' = \frac{P'(P+D)}{\Delta} = \frac{P'}{\Delta} \left( P + \frac{P^2 + \Delta}{E} \right) = P' \left( \frac{P}{\Delta} + \frac{P^2}{\Delta E} + \frac{1}{E} \right).$$

But  $\Delta \geq 1$  and  $E \geq 2$ , so

$$r' \leq P' \left( P + \frac{P^2}{2} + \frac{1}{2} \right) = \frac{1}{2} P' (P+1)^2,$$

with equality iff  $\Delta = 1$  and  $E = 2$ , which from (2.9a) and (3.1) occurs iff  $q' = P'(P+2)$ , whence the result.  $\square$

**Theorem 3.3.** *For any  $KN$ ,  $n \leq N_3(P) := \frac{1}{2}(P^6 + 2P^5 - P^4 - P^3 + 2P^2 - P)$ , with equality iff  $q = Q_3(P) = P^2 + P - 1$  and  $r = R_3(P) = \frac{1}{2}(P-1)(P+1)^2 + 1$ .*

*Proof.* For  $\Delta \geq 2$ , from (3.1),  $q \leq P^2 - \frac{3}{2}P + \frac{3}{2} < Q_3(P)$  for  $P \geq 3$ , and from Theorem 3.2,  $r < R_3(P)$ , so  $n < P \cdot Q_3(P) \cdot R_3(P)$ .

For  $\Delta = 1$  and given  $P$ , with  $\eta$  and  $n$  real variables, from (2.15)  $n$  is greatest when  $\eta$  is greatest. But from (2.11)

$$\eta = \frac{\Delta + s^2}{P - s} = \frac{s^2 + 1}{P - s},$$

and  $1 \leq s \leq P-2$ , giving maximum  $\eta = \frac{1}{2}(P^2 - 4P + 5)$  when  $s = P-2$ , i.e.  $E = 2$  from (2.10). But from Theorem 3.2, for  $\Delta = 1$  and  $E = 2$  we have  $q = Q_3(P)$  and  $r = R_3(P)$ , so  $n \leq P \cdot Q_3(P) \cdot R_3(P)$ , which multiplies out to give the result.  $\square$

Beeger [2] for  $d = 3$  and Duparc [9] for any  $CN$  proved results similar to Theorem 3.1 and weaker than Theorem 3.2. They were chiefly concerned to show that the number of  $CN$ 's for given  $P$  is finite. Swift stated the first result of Theorem 3.3 for  $d = 3$  in 1975, but his proof is not published in [17].

For a  $K_3$ -family attaining these upper bounds for  $r$  and  $n$  given  $P$ , we simply put  $P = 2t + 1$  in  $n = N_3(P) = P \cdot Q_3(P) \cdot R_3(P)$ . We note that  $Q_2(3) = Q_3(3) = 11$  and  $R_2(3) = R_3(3) = 17$ , so the smallest  $CN$  (and  $KN$ , easily shown),  $n = 561$ , uniquely is  $q$ -maximal,  $r$ -maximal and  $n$ -maximal.  $N_3(P)$  gives  $C_3N$ 's for  $P = 3, 5, 31, 41, 83, 131, \dots$ ; and  $N_3(65) = 5 \cdot 13 \cdot 4289 \cdot 139393 = 38860677505$  is the smallest  $r$ - $n$ -maximal  $C_4N$  for given  $P$ . A computer search over  $3 \leq P \leq 132425$  found 178  $C_3N$ 's, 18  $C_4N$ 's, 29  $C_5N$ 's and 9  $C_6N$ 's which are  $r$ - $n$ -maximal, the largest of which is the  $C_3N$  with  $P = 131711$ .

**3.2. Upper bounds given  $n$  for  $P, q, r$ .** For an upper bound for  $P$  given  $n$ , we do not attempt to improve on the obvious:

**Theorem 3.4.** *For any  $KN$ ,  $P < n^{\frac{d-2}{d}}$*

*Proof.* We have  $p_1 < p_2 < \dots < p_{d-2} < q < r$  (with obvious modification for  $d < 5$ ). Hence  $P = \prod_{i=1}^{d-2} p_i \leq p_{d-2}^{d-2}$ , so  $p_{d-2} \geq P^{\frac{1}{d-2}}$  and  $P = \frac{n}{qr} < \frac{n}{p_{d-2}^2} \leq \frac{n}{P^{\frac{2}{d-2}}}$ .

Hence  $P^{\frac{d}{d-2}} < n$  and the result follows.  $\square$

It seems plausible that an upper bound for  $q$  given  $n$  should correspond to the Theorem 3.1 bound for  $q$  given  $P$ , so in terms of (3.3) and (3.4) we should have

**Theorem 3.5.** *For any  $KN$ ,  $q \leq Q_2(N_2^{-1}(n)) = q_2(n_2^{-1}(n))$ , with equality iff*

$$q = Q_2(P) = \left(P - 1\right) \left(2P + \frac{1}{2} - \sqrt{P - \frac{3}{4}}\right) + 1$$

*Explicitly,*

$$q \leq \left\lfloor \sqrt[5]{2n^2} - \sqrt[10]{\frac{n^3}{64}} - \frac{1}{10} \sqrt[5]{\frac{n}{4}} + \frac{17}{20} \sqrt[10]{\frac{n}{4}} \right\rfloor$$

*Proof.* If  $V = N_2^{-1}(n)$ , the substitution  $V = v^2 + v + 1$  with the algebra of (3.3) and (3.4) establishes the equivalence of the functions  $Q_2 N_2^{-1}$  and  $q_2 n_2^{-1}$ , and if  $\Delta = \eta = 1$  it is immediate that  $q = Q_2(N_2^{-1}(n))$ ; also  $\Delta = \eta = 1$  for  $n = 561$ , the only  $KN$  with  $P = 3$ . So we assume  $KN$ 's with  $\Delta\eta \geq 2$  and  $P \geq 5$ , and we consider two cases: (i)  $\Delta \geq P'$ , (ii)  $1 \leq \Delta \leq P - 2$ . We write  $\lambda := \frac{P'}{\Delta}$ .

(i)  $\lambda \leq 1$ . From (2.13b) and (2.14a),  $q' = \lambda(2P - s) < 2\lambda P$ , and then from (2.15)  $n = P\{\lambda^2(4P^2 + \eta P + \Delta) + \lambda(4P + \eta) + 1\} > 4\lambda^2 P^3 > 4\lambda^2 (\frac{q'}{2\lambda})^3 = \frac{q'^3}{2\lambda}$ . Hence  $q'^3 < 2\lambda n \leq 2n$ , so  $q < (2n)^{\frac{1}{3}} + 1$ . Let  $v := n_2^{-1}(n)$ , so  $n = n_2(v)$ , and it is easily verified that  $(2n_2(v))^{\frac{1}{3}} + 1 < q_2(v)$  for  $v \geq 1.1$ . But  $n_2(1.1) < 963$  and every  $KN$  with  $P \geq 5$  has  $n \geq 1105 = 5 \cdot 13 \cdot 17$  and hence  $v \geq 1.1$ , so  $q < q_2(n_2^{-1}(n))$  as required.

(ii)  $\lambda > 1$ . Let  $n_o$  be any particular  $KN$  with associated  $K$ -variable values  $P_o, q_o, n_o, \Delta_o, \eta_o, \theta_o, s_o$  and  $\lambda_o = \frac{P_o'}{\Delta_o} > 1$ . We define  $s, \theta, q, r$  and  $n$  as functions of independent real variables  $P, \Delta, \eta$  by the formulae of (2.12-2.15) over the domain  $3 \leq P \leq P_o$ ,  $1 \leq \eta \leq \eta_o$  and  $1 \leq \Delta \leq \Delta_o$  with  $\Delta < P$  (ensuring  $\theta \in \mathbb{R}$ ), and we write  $n = n(P, \Delta, \eta)$  with  $n_o = n(P_o, \Delta_o, \eta_o)$ , etc. Then, if  $\eta_o > 1$ , over the interval  $1 < \eta < \eta_o$  from (2.14a), (3.2) and (2.15) we have  $\frac{\partial q}{\partial \eta} < 0$  and  $\frac{\partial n}{\partial \eta} > 0$ , whence  $q_a := q(P_o, \Delta_o, 1) \geq q_o$  and  $n_a := n(P_o, \Delta_o, 1) \leq n_o$ , with equality iff  $\eta_o = 1$ . In what follows we use the suffices “a” and “b” to correspond to “states”  $(\Delta, \eta) = (\Delta_o, 1)$  and  $(\Delta, \eta) = (1, 1)$  respectively.

Then, if  $\Delta_o > 1$ , for  $1 \leq \Delta \leq \Delta_o$  we define the function  $P = P^*(\Delta)$  implicitly via the relation  $n(P, \Delta, 1) = n_a$ , so  $n_a = n_b$  and

$$(3.5) \quad P \left\{ \frac{P'^2}{\Delta^2} (4P^2 + P) + 5 \frac{P'P}{\Delta} + 1 \right\} = P \{ \lambda^2 P (4P + 1) + 5\lambda P + 1 \} = n_a, \text{ constant,}$$

and as  $\Delta$  decreases from  $\Delta_o$  to 1 we see from the first of these expressions that  $P$  steadily decreases, whence from the second  $\lambda$  steadily increases. So, for  $\Delta_o > \Delta > 1$ ,  $\frac{P'}{\Delta} = \lambda > \lambda_o > 1$ , whence  $P - \Delta > 1$ , so  $\theta = \sqrt{4(P - \Delta) + 1} > \sqrt{5}$ , ensuring that, via (2.13) and (2.14) with  $\eta = 1$ ,  $\theta^*(\Delta) := \theta(P^*(\Delta), \Delta, 1) = \theta$ , and, similarly,



$q^*(\Delta) = q$  and  $r^*(\Delta) = r$  are defined for  $1 \leq \Delta \leq \Delta_o$ ; also  $P > \Delta + 1 > 2$ , so certainly  $N_2(P)$  is an increasing function over the relevant domain. Now, for  $\Delta_o \geq 1$ , write  $P_b := P^*(1) = N_2^{-1}(n_a)$ , so since by hypothesis  $P_o \geq 5$  and  $\lambda_o > 1$ , we have

$$\begin{aligned} N_2(P_b) &= n(P_b, 1, 1) = n_a = n(P_o, \Delta_o, 1) \\ &= P_o \{ \lambda_o^2 (4P_o^2 + P_o) + 5\lambda_o P_o + 1 \} > 4P_o^3 + 6P_o^2 + P_o \geq 655 > 561 = N_2(3), \end{aligned}$$

whence  $P_b > 3$ ; but  $P \geq P^*(1) = P_b$ , so  $P > 3$ . Thus from the above we have

$$(3.6) \quad \text{For } 1 < \Delta < \Delta_o, \quad \lambda > 1, \quad P > 3 \text{ and } \theta > \sqrt{5}.$$

Also let  $s_b := p_2^{-1}(P_b) = \frac{1}{2}(\sqrt{4P_b - 3} - 1)$  and  $q_b := Q_2(P_b) = q_2(s_b)$ , so if  $\Delta_o = 1$  then  $q_b = q_a$ .

Next we shall show that, with  $\eta = 1$ ,  $\frac{dq}{d\Delta} < 0$  for  $1 < \Delta < \Delta_o$ , and then since  $Q_2, q_2, N_2$  and  $n_2$  are all increasing functions over the relevant domains, we shall have  $q^*(\Delta_o) \leq q^*(1)$ , and so  $q_o \leq q_a = q(P_o, \Delta_o, 1) = q^*(\Delta_o) \leq q^*(1) = q(P_b, 1, 1) = q_b = Q_2(P_b) = Q_2(N_2^{-1}(n_a)) \leq Q_2(N_2^{-1}(n_o))$ , and likewise  $q_o \leq q_b = q_2(s_b) \leq q_2(n_o^{-1}(n_o))$ , with equality throughout iff  $\Delta_o = \eta_o = 1$ , i.e. iff  $q_o = Q_2(P_o)$  as required.

From the first of the two expressions for  $n_a$  in (3.5) we have

$$(3.7) \quad qr = \frac{P'^2(4P^2 + P)}{\Delta^2} + \frac{5(P^2 - P)}{\Delta} + 1$$

$$\therefore \frac{d(qr)}{d\Delta} = \frac{1}{\Delta^2} \{ 2P'(4P^2 + P) + P'^2(8P + 1) \} \frac{dP}{d\Delta} - \frac{2P'^2(4P^2 + P)}{\Delta^3} + \frac{5(2P - 1)}{\Delta} \frac{dP}{d\Delta} - \frac{5PP'}{\Delta^2}, \quad \text{that is}$$

$$(3.8) \quad \frac{d(qr)}{d\Delta} = \left\{ \frac{P'(16P^2 - 5P - 1)}{\Delta^2} + \frac{5(2P - 1)}{\Delta} \right\} \frac{dP}{d\Delta} - \frac{2PP'^2(4P + 1)}{\Delta^3} - \frac{5PP'}{\Delta^2}$$

$$\text{But } Pqr = n_a, \text{ constant, so } qr \frac{dP}{d\Delta} + P \frac{d(qr)}{d\Delta} = 0;$$

substituting from (3.7) and (3.8) gives

$$\begin{aligned} & \left\{ \frac{P'^2 P(4P + 1)}{\Delta^2} + \frac{5PP'}{\Delta} + 1 + \frac{PP'(16P^2 - 5P - 1)}{\Delta^2} + \frac{5P(2P - 1)}{\Delta} \right\} \frac{dP}{d\Delta} \\ &= \frac{2P^2 P'^2(4P + 1)}{\Delta^3} + \frac{5P^2 P'}{\Delta^2}, \quad \text{whence} \end{aligned}$$

$$(3.9) \quad \Delta \left\{ 2P'(10P^2 - 4P - 1) + 5\Delta(3P - 2) + \frac{\Delta^2}{P} \right\} \frac{dP}{d\Delta} = 2PP'^2(4P + 1) + 5\Delta PP'$$

Also with  $\eta = 1$ , (2.14a) gives  $2q = \frac{P'}{\Delta}(4P + 1 - \theta) + 2$  and from (2.13a)  $\theta^2 = 4P + 1 - 4\Delta$ , so  $\theta = \frac{1}{\theta}(4P + 1 - 4\Delta)$ ,

$$\frac{d\theta}{d\Delta} = \frac{2}{\theta} \left( \frac{dP}{d\Delta} - 1 \right) \quad \text{and} \quad 2 \frac{dq}{d\Delta} = \left( \frac{1}{\Delta} \frac{dP}{d\Delta} - \frac{P'}{\Delta^2} \right) (4P + 1 - \theta) + \frac{P'}{\Delta} \left( 4 \frac{dP}{d\Delta} - \frac{d\theta}{d\Delta} \right).$$

Hence  $2\Delta^2 \frac{dq}{d\Delta} = \left( \Delta \frac{dP}{d\Delta} - P' \right) \left( 4P + 1 - \frac{4P + 1}{\theta} + \frac{4\Delta}{\theta} \right) + \Delta P' \left( 4 \frac{dP}{d\Delta} - \frac{2}{\theta} \frac{dP}{d\Delta} + \frac{2}{\theta} \right)$ , i.e.

$$(3.10) \quad 2\Delta^2 \frac{dq}{d\Delta} = \Delta \left\{ 8P - 3 - \frac{6P - 1}{\theta} + \frac{4\Delta}{\theta} \right\} \frac{dP}{d\Delta} - P' \left( 4P + 1 \right) \left( 1 - \frac{1}{\theta} \right) - \frac{2\Delta P'}{\theta}$$

Writing  $M := 2P'(10P^2 - 4P - 1) + 5\Delta(3P - 2) + \frac{\Delta^2}{P}$ , from (3.9) and (3.10) we get

$$\begin{aligned} -2\Delta^2 M \frac{dq}{d\Delta} &= \left\{ P' \left( 4P + 1 \right) \left( 1 - \frac{1}{\theta} \right) + \frac{2\Delta P'}{\theta} \right\} \left\{ 2P'(10P^2 - 4P - 1) + 5\Delta(3P - 2) + \frac{\Delta^2}{P} \right\} \\ &\quad - \left\{ 8P - 3 - \frac{6P - 1}{\theta} + \frac{4\Delta}{\theta} \right\} \left\{ 2PP'^2(4P + 1) + 5\Delta PP' \right\} \end{aligned}$$

The coefficient of  $\frac{\Delta}{\theta}$  in this expression is

$$\begin{aligned} &P' \{ 4P'(10P^2 - 4P - 1) - 5(4P + 1)(3P - 2) + 5P(6P - 1) - 8PP'(4P + 1) \} \\ &= P' \{ 4P'(2P^2 - 6P - 1) - 5(6P^2 - 4P - 2) \} = 2P'^2 \{ 2(2P^2 - 6P - 1) - 5(3P + 1) \} \\ &= 2P'^2(4P^2 - 27P - 7) = 2P'^2(4P + 1)(P - 7) \end{aligned}$$

and of  $\frac{\Delta^2}{\theta}$  is

$$P' \left\{ -\frac{4P + 1}{P} + 10(3P - 2) - 20P \right\} = \frac{P'(10P^2 - 24P - 1)}{P},$$

so

$$\begin{aligned} -2\Delta^2 M \frac{dq}{d\Delta} &= 2P'^2(4P + 1)(2P^2 - P - 1) + 5\Delta P'(4P^2 - 2P - 2) + \frac{\Delta^2 P'(4P + 1)}{P} \\ &\quad - \frac{2P'^2(4P + 1)}{\theta} \{ 4P^2 - 3P - 1 \} + \frac{2\Delta P'^2(4P + 1)(P - 7)}{\theta} \\ &\quad + \frac{\Delta^2 P'(10P^2 - 24P - 1)}{\theta P} + \frac{2\Delta^3 P'}{\theta P} \end{aligned}$$

Factorising terms and dividing by  $2P'^3(4P + 1)$  gives

$$\begin{aligned} -\frac{\Delta^2 M}{(4P + 1)P'^3} \frac{dq}{d\Delta} &= W := 2P + 1 + \frac{5\Delta(2P + 1)}{P'(4P + 1)} + \frac{\Delta^2}{2PP'^2} - \frac{(4P + 1)}{\theta} \\ &\quad + \frac{\Delta(P - 7)}{\theta P'} + \frac{\Delta^2(10P^2 - 24P - 1)}{2\theta PP'^2(4P + 1)} + \frac{\Delta^3}{\theta PP'^2(4P + 1)} \end{aligned}$$

From (3.6)  $P > 3$  and  $\theta > \sqrt{5}$ , so  $M > 0$  and also  $10P^2 - 24P - 1 > 0$ , whence

$$\begin{aligned} W &> 2P + 1 - \frac{4P + 1}{\theta} + \frac{5(2P + 1)}{\lambda(4P + 1)} + \frac{P - 7}{\lambda\theta} \\ &= \frac{(2\theta - 4)P + \theta - 1}{\theta} + \frac{(4P + 1)(P - 7) + 5\theta(2P + 1)}{\lambda\theta(4P + 1)} \\ &> \frac{(4P + 1)(P - 7) + 5\sqrt{5}(2P + 1)}{\lambda\theta(4P + 1)} = \frac{4P^2 + (10\sqrt{5} - 27)P + 5\sqrt{5} - 7}{\lambda\theta(4P + 1)} > 0 \end{aligned}$$

since the discriminant of the numerator is negative.

Hence  $\frac{dq}{d\Delta} = -\frac{(4P + 1)\lambda^2 P' W}{M} < 0$  as required, completing the proof of the first part of the theorem.

We now outline a method of expressing  $Q_2(N_2^{-1}(n))$  as a power series in  $\frac{1}{\sqrt[10]{n}}$ . Let  $U := \sqrt[5]{\frac{n}{4}}$ , and (3.2) becomes

$$(3.11) \quad U^5 = P^5 - \frac{7}{4}P^4 + \frac{7}{4}P^3 - P^2 + \frac{1}{4}P$$

and if we now put  $P = U + B_o + \frac{B_1}{U} + \frac{B_2}{U^2} + \dots$ , substitute into (3.11) and equate coefficients of  $U^{1-k}$  to find successively  $B_o, B_1, B_2, \dots$ , we obtain

$$(3.12) \quad P = U + \frac{7}{20} - \frac{21}{200U} + \frac{1}{250U^2} + \frac{2787}{160000U^3} + \dots$$

To find

$$\begin{aligned} Q_2(N_2^{-1}(n)) &= Q_2(P) = P' \left( 2P + \frac{1}{2} - \sqrt{P - \frac{3}{4}} \right) + 1 \\ &= 2PP' + \frac{P'}{2} - P' \sqrt{P - \frac{3}{4}} + 1, \end{aligned}$$

and with  $u = \sqrt{U} = \sqrt[10]{\frac{n}{4}}$ , from (3.12) we have

$$P = u^2 + \frac{7}{20} - \frac{21}{200u^2} + \frac{1}{250u^4} + \dots, \quad P' = u^2 - \frac{13}{20} - \frac{21}{200u^2} + \frac{1}{250u^4} + \dots \quad \text{and}$$

$$\begin{aligned} \sqrt{P - \frac{3}{4}} &= \left( u^2 - \frac{2}{5} - \frac{21}{200u^2} + \frac{1}{250u^4} + \dots \right)^{\frac{1}{2}} = u \left[ 1 - \left( \frac{2}{5u^2} + \frac{21}{200u^4} - \frac{1}{250u^6} + \dots \right) \right]^{\frac{1}{2}} \\ &= u - \frac{1}{5u} - \frac{29}{400u^3} - \frac{1}{80u^5} + \dots, \end{aligned}$$

after applying the binomial series and simplifying.

Substituting back, we get

$$Q_2(P) = 2u^4 - u^3 - \frac{u^2}{10} + \frac{17u}{20} - \frac{1}{5} + \frac{19}{400u} + \frac{53}{2000u^2} - \frac{477}{8000u^3} + \dots$$

If now the variables all belong to a  $KN$ , then  $q = Q_2(P)$  is an integer and  $q = \lfloor 2u^4 - u^3 - 0.1u^2 + 0.85u \rfloor$ , and Theorem 3.5 follows.  $\square$

Much more simply, we now establish an upper bound for  $r$  given  $n$ ; first we prove

**Theorem 3.6.** *For any  $KN$ ,*

$$p_i = \frac{\lambda_i' + \sqrt{\lambda_i'^2 + 4\lambda_i n}}{2\lambda_i} = \left\lceil \sqrt{\frac{n}{\lambda_i}} \right\rceil$$

*Proof.* Using the notation of §2.1, we have

$$p_i p_i' = \frac{p_i P_i'}{\lambda_i} = \frac{n}{\lambda_i} - \frac{p_i}{\lambda_i}, \quad \text{whence}$$

$$(3.13) \quad \frac{n}{\lambda_i} = p_i^2 - \left( 1 - \frac{1}{\lambda_i} \right) p_i$$

and  $\lambda_i p_i^2 - \lambda_i' p_i - n = 0$ , giving the first equality.

Also  $\lambda_i \geq E \geq 2$ , so  $0 < 1 - \frac{1}{\lambda_i} < 1$ , and from (3.13) we thus have

$$(p_i - 1)^2 < \frac{n}{\lambda_i} < p_i^2, \quad \text{so} \quad p_i = \left\lceil \sqrt{\frac{n}{\lambda_i}} \right\rceil$$

completing the theorem.  $\square$

**Theorem 3.7.** *For any  $KN$ ,*

$$r \leq \frac{\sqrt{8n+1}+1}{4} \quad \text{and} \quad r \leq \left\lceil \sqrt{\frac{n}{2}} \right\rceil, \quad \text{with equality iff } E = 2.$$

*Proof.* This follows easily from Theorem 3.6.

$n \geq 561$  and  $n$  is odd, so with  $i = d$  in Theorem 3.6 and  $\lambda_d = E \geq 3$ , we have

$$r = \left\lceil \sqrt{\frac{n}{E}} \right\rceil < \sqrt{\frac{n}{E}} + 1 < \sqrt{\frac{n}{2}} < \left\lceil \sqrt{\frac{n}{2}} \right\rceil \quad \text{and} \quad \sqrt{\frac{n}{2}} < \frac{\sqrt{8n+1}+1}{4};$$

in conjunction with  $E = 2$  in Theorem 3.6, Theorem 3.7 follows.  $\square$

The smallest  $CN$  which is  $r$ -maximal for given  $n$  but not for given  $P$  (see Theorem 3.2) is  $8911 = 7 \cdot 19 \cdot 67$ . Another of this type is  $949803513811921 = 17 \cdot 31 \cdot 191 \cdot 433 \cdot 21792241$ , which Pinch in [12] says contains the largest prime factor among  $CN$ 's  $< 10^{15}$ .

#### 4. BOUNDS FOR $K_3N$ VARIABLES

**4.1. Upper bounds given  $p$  for  $A, B, C$ .** To establish an upper bound for  $A$  given  $p$ , we need one for  $A$  given  $H$ :

**Theorem 4.1.** *For any  $K_3N$ ,  $A < 3H - \sqrt{\frac{H}{2}}$ .*

*Proof.* Suppose for some  $K_3N$  that  $A \geq \lambda H$  for some  $\lambda > 0$ . Then (2.5b) yields

$$\begin{aligned} F &\leq H \left( \frac{1}{\lambda H} + \frac{1}{\lambda H + 1} + \frac{1}{\lambda H + 2} \right) + \frac{1}{\lambda H(\lambda H + 1)} + \frac{1}{\lambda H(\lambda H + 2)} + \frac{1}{(\lambda H + 1)(\lambda H + 2)} \\ &= \frac{1}{\lambda} + \left( \frac{1}{\lambda} - \frac{1}{\lambda(\lambda H + 1)} \right) + \left( \frac{1}{\lambda} - \frac{2}{\lambda(\lambda H + 2)} \right) + \frac{3\lambda H + 3}{\lambda H(\lambda H + 1)(\lambda H + 2)} \\ &= \frac{3}{\lambda} - \frac{3\lambda H(H - 1) + 4H - 3}{\lambda H(\lambda H + 1)(\lambda H + 2)} < \frac{3}{\lambda} \quad \text{since } H \geq 2 \end{aligned}$$

But  $F \geq 1$ , so putting  $\lambda = 3$  we get  $A < 3H$ . Also if  $\lambda = \frac{3}{2}$  then  $F < 2$ , whence if  $\frac{3H}{2} \leq A < 3H$ , then  $F = 1$ . We define a big- $A$ - $K_3N$  to be a  $K_3N$  with  $A \geq \frac{3H}{2}$ , and likewise a big- $A$ - $C_3N$ . All other  $K_3N$ 's obviously obey Theorem 4.1.

So we now put  $A = 3H - a$ , with  $1 \leq a \leq \frac{3H}{2}$ , and using  $F = 1$  we shall show that for given  $a$ ,  $H < 2a^2$ , yielding Theorem 4.1. We write  $\alpha := -a$ ,  $A = 3H + \alpha$ ,  $B = 3H + \beta$ ,  $C = 3H + \gamma$ ,  $\sigma := \frac{\beta + \gamma}{2}$ ,  $\tau := \frac{\gamma - \beta}{2}$ , so  $\beta\gamma = \sigma^2 - \tau^2$ , and  $S := \sum \alpha = 2\sigma - a$ . Then for a  $K_3N$  we have  $-a = \alpha < \beta = \sigma - \tau < \gamma$ , so  $0 < \tau < a + \sigma$ , and from (2.5)

$$F = \frac{(\sum AB)H + \sum A}{ABC} = \frac{27H^3 + 6(\sum \alpha)H^2 + (\sum \alpha\beta + 9)H + \sum \alpha}{27H^3 + 9(\sum \alpha)H^2 + 3(\sum \alpha\beta)H + \alpha\beta\gamma} = 1 - \frac{m}{ABC}$$

where

$$(4.1a) \quad m := m(H) := 3(\sum \alpha)H^2 + (2\sum \alpha\beta - 9)H + \alpha\beta\gamma - \sum \alpha$$

$$(4.1b) \quad = 3SH^2 + (2\sigma^2 - 2\tau^2 - 4a\sigma - 9)H - a(\sigma^2 - \tau^2 - 1) - 2\sigma$$

So for any  $K_3N$ ,  $F = 1$  iff  $m = 0$ , and  $A = 3H - a > 0$ , so  $H > \frac{a}{3}$ ; also for any big- $A$ - $K_3N$ ,  $\gamma > 0$  (since otherwise

$$\frac{H}{C} = \frac{H}{3H + \gamma} \geq \frac{1}{3} \quad \text{and so} \quad F > \sum \frac{H}{3H + \alpha} > 1, \text{ but } F = 1).$$

We now regard  $m(H)$  and  $F(H) := 1 - \frac{m(H)}{(3H + \alpha)(3H + \beta)(3H + \gamma)}$  as functions

of an unrestricted real variable  $H$ , where  $\alpha, \beta, \gamma$  are real,  $\alpha < 0 < \gamma$  and  $\alpha \leq \beta \leq \gamma$ . Essentially by considering the graph of  $F(H)$ , we show that  $m(H) = 0$  has a root  $H^* > \frac{a}{3} = -\frac{\alpha}{3}$  iff  $S > 0$ . We have

$$\begin{aligned} m(-\frac{\alpha}{3}) &= (\alpha + \beta + \gamma) \frac{\alpha^2}{3} - \{2\alpha(\beta + \gamma) + 2\beta\gamma - 9\} \frac{\alpha}{3} + \alpha\beta\gamma - (\alpha + \beta + \gamma) \\ &= \frac{\alpha}{3} \{\alpha^2 - \alpha(\beta + \gamma) + \beta\gamma\} + 2\alpha - \beta - \gamma \\ &= \frac{\alpha}{3} (\alpha - \beta)(\alpha - \gamma) + (\alpha - \beta) + (\alpha - \gamma), \end{aligned}$$

with similar results for  $m(-\frac{\beta}{3})$  and  $m(-\frac{\gamma}{3})$ , whence  $m(-\frac{\alpha}{3}) < 0$  and  $m(-\frac{\gamma}{3}) > 0$ . First we show that in all cases  $m(H) = 0$  has a root  $h^*$  satisfying  $-\frac{\gamma}{3} < h^* < -\frac{\alpha}{3}$ .

$$(4.2) \quad \text{As } H \rightarrow -\frac{\gamma}{3} - \text{ and as } H \rightarrow -\frac{\alpha}{3} +, \quad F(H) \rightarrow \infty$$

Then if  $\beta = \gamma$ , as  $H \rightarrow -\frac{\gamma}{3} +$ ,  $F(H) \rightarrow \infty$ ; as  $H \rightarrow -\frac{\alpha}{3} -$ ,  $F(H) \rightarrow -\infty$ ; and  $F(H)$  is continuous over the interval  $(-\frac{\gamma}{3}, -\frac{\alpha}{3})$ , so there exists  $h^* \in (-\frac{\gamma}{3}, -\frac{\alpha}{3})$  with  $F(h^*) = 1$  and  $m(h^*) = 0$  as required; and similarly if  $\beta = \alpha$ . Also if  $\alpha < \beta < \gamma$  and (a)  $m(-\frac{\beta}{3}) \neq 0$ , then as  $H \rightarrow -\frac{\gamma}{3} +$  and as  $H \rightarrow -\frac{\alpha}{3} -$ ,  $F(H) \rightarrow -\infty$ , and  $F(H)$  changes sign as  $H$  increases through the singularity at  $H = -\frac{\beta}{3}$ , so again there exists  $h^*$  with  $F(h^*) = 1$  and  $m(h^*) = 0$  in at least one of the intervals  $(-\frac{\gamma}{3}, -\frac{\beta}{3})$  and  $(-\frac{\beta}{3}, -\frac{\alpha}{3})$ , and so in  $(-\frac{\gamma}{3}, -\frac{\alpha}{3})$ ; while (b) if  $m(-\frac{\beta}{3}) = 0$  then  $h^* = -\frac{\beta}{3}$ . Hence  $m(H)$  has at least one zero  $h^* \in (-\frac{\gamma}{3}, -\frac{\alpha}{3})$ , as required. Then, if  $S = 0$ ,  $m(H)$  is linear and  $h^*$  is the only root. But, if  $S > 0$ ,  $m(H)$  is quadratic and as  $H \rightarrow \infty$ ,  $F(H) \rightarrow 1 -$ , so with (4.2) this gives  $H^* > -\frac{\alpha}{3}$  such that  $F(H^*) = 1$  and thus a unique second root  $H^*$  of  $m(H) = 0$  with  $H^* > \frac{a}{3}$ . Similarly for  $S < 0$ , the second root  $H^*$  satisfies  $H^* < -\frac{\gamma}{3} < 0$ , and hence  $H^* > \frac{a}{3}$  iff  $S > 0$ , as required (in fact  $H^* > \frac{a}{2}$ , else  $F(H^*) > 1$ , as is easily seen).

Assuming henceforth that  $S > 0$ , from the above argument for  $H > \frac{a}{3}$  we have  $F(H) > F(H^*) = 1$  iff  $H < H^*$ . So if, with obvious notation, for  $(\alpha_i, \beta_i, \gamma_i)$ ,  $\alpha_1 = \alpha_2 = -a$ , and for every  $H > \frac{a}{3}$  we have  $F_1(H) > F_2(H)$ , then  $F_1(H_2^*) > F_2(H_2^*) = 1 = F_1(H_1^*)$ , so  $H_2^* < H_1^*$ . In particular we deduce that

(i) if  $\alpha_1 = \alpha_2$ ,  $\beta_1 \leq \beta_2$ ,  $\gamma_1 \leq \gamma_2$ , with at least one strict inequality, then  $H_2^* < H_1^*$ ;

(ii) if  $\alpha_1 = \alpha_2 = -a$  and  $S_1 = S_2 = S$  (so  $\sigma_1 = \sigma_2 = \sigma = \frac{a+S}{2}$ ), but  $\tau_1 > \tau_2$ , then  $H_2^* < H_1^*$ , i.e for fixed  $a$ ,  $S$  and  $\sigma$ ,  $H^*$  increases as  $\tau$  increases. This follows because  $(\alpha, \beta, \gamma) = (\alpha, \sigma - \tau, \sigma + \tau)$  and

$$F(H) = H \sum \frac{1}{A} + \sum \frac{1}{AB} = \frac{H}{A} + \frac{1}{BC} \left\{ \left( H + \frac{1}{A} \right) (B + C) + 1 \right\};$$

but  $B + C = 6H + 2\sigma$  and  $BC = (3H + \sigma)^2 - \tau^2$ ; so for  $H > \frac{a}{3}$ ,  $F_1(H) > F_2(H)$  and  $H_2^* < H_1^*$ .

We write  $H^\dagger(a, S, \tau) := H^*(\alpha, \beta, \gamma) := H^*$ , and  $h(\beta, \gamma) := H^*(-1, \beta, \gamma)$ . We observe that for a bigA- $K_3N$ ,  $H = H^*$ , and that  $A, B, C$  pairwise coprime and  $H$  even requires that no two of  $\alpha, \beta, \gamma$  are even; so, since  $\beta + \gamma = S + a$ ,  $S$  odd requires  $\alpha, \beta, \gamma$  all odd. We now show that for any bigA- $K_3N$ ,  $H < 2a^2$ , considering cases (a)  $a = 1$ , (b)  $a \geq 2$ ,  $S = 1$ , and (c)  $a \geq 2$ ,  $S \geq 2$ .

(a) Any  $K_3N$  with  $a = 1$  is a bigA- $K_3N$ . So  $\alpha = -1$ , and for  $\beta = 0$ , since  $S > 0$  and  $B, C$  are coprime,  $\gamma \geq 5$  and from (4.1a) and (i) above we have  $h(0, \gamma) \leq h(0, 5) \simeq 1.68 < 2 \leq H$ . Also for  $\beta \geq 2$ , by (i) we have

$h(\beta, \gamma) < h(1, \gamma) \leq h(1, 3) \simeq 1.63 < 2$ , covering all cases except  $h(1, 2) \simeq 2.14 \notin 2\mathbb{N}$ . Thus there are no  $K_3N$ 's with  $a = 1$ .

(b) We have  $S = 1$ , odd, so  $a$  is odd and  $a \geq 3$ . Then maximum  $\tau$  for given  $a$  occurs when  $(\alpha, \beta, \gamma) = (-a, -a + 2, 2a - 1)$ , giving  $\tau = \frac{3a-3}{2}$ ; and from (ii) above  $H \leq g := g(a) := H^\dagger(a, 1, \frac{3a-3}{2})$ , which from (4.1a) is given by

$$\begin{aligned} 3g^2 - (6a^2 - 8a + 13)g + 2a^3 - 5a^2 + 2a - 1 &= 0, \quad \text{whence} \\ \text{i.e.} \quad g &= \frac{1}{6}(6a^2 - 8a + 13 + \sqrt{36a^4 - 120a^3 + 280a^2 - 244a + 181}), \\ (4.3) \quad H \leq g(a) &= \frac{1}{6}(6a^2 - 8a + 13 + \sqrt{(6a^2 - 10a + 15)^2 + 68a - 44}) \\ &< 2a^2 \quad \text{for } a \geq 3. \end{aligned}$$

(c) First we find  $H^\dagger(a, S, a + \sigma) = H^*(-a, -a, 2a + S)$ , which from (4.1b) is the root  $H^*$  of  $3SH^2 - (2a^2 + 8a\sigma + 9)H + a^3 + 2a^2\sigma - 2\sigma + a = 0$ , which has

$$\begin{aligned} \text{discriminant} &= (2a^2 + 8a\sigma + 9)^2 - 12(2\sigma - a)(a^3 + 2a^2\sigma - 2\sigma + a) \\ &= 16a^4 + 32a^3\sigma + 16a^2\sigma^2 + 48a^2 + 96a\sigma + 48\sigma^2 + 81 \\ &= 16(a^2 + 3)(a + \sigma)^2 + 81 \quad \text{and hence} \end{aligned}$$

$$(4.4a) \quad H^\dagger(a, S, a + \sigma) = \frac{1}{6S}(2a^2 + 8a\sigma + 9 + \sqrt{16(a^2 + 3)(a + \sigma)^2 + 81})$$

$$(4.4b) \quad = \frac{1}{6S}(2a^2 + 4a(a + S) + 9 + \sqrt{4(a^2 + 3)(3a + S)^2 + 81})$$

$$(4.4c) \quad = \frac{a^2}{S} + \frac{2a}{3} + \frac{3}{2S} + \sqrt{(a^2 + 3)\left(\frac{a}{S} + \frac{1}{3}\right)^2 + \frac{9}{4S^2}}$$

So from (i) or (4.4c) for given  $a$ ,  $H^\dagger(a, S, a + \sigma)$  decreases as  $S$  increases, and hence for any bigA- $K_3N$  with  $S \geq 2$  and  $a \geq 2$ , also using (ii) we have

$$H = H^\dagger(a, S, \tau) < H^\dagger(a, S, a + \sigma) \leq H^\dagger\left(a, 2, \frac{3a+2}{2}\right),$$

and from (4.4b) we have

$$\begin{aligned} H^\dagger\left(a, 2, \frac{3a+2}{2}\right) &< 2a^2 \Leftrightarrow \sqrt{(a^2 + 3)\left(\frac{a}{2} + \frac{1}{3}\right)^2 + \frac{9}{16}} < \frac{3}{2}a^2 - \frac{2a}{3} - \frac{3}{4} \\ &\Leftrightarrow \frac{a^4}{4} + \frac{a^3}{3} + \left(\frac{3}{4} + \frac{1}{9}\right)a^2 + a + \frac{1}{3} < \frac{9}{4}a^4 - 2a^3 + \left(\frac{4}{9} - \frac{9}{4}\right)a^2 + a \\ &\Leftrightarrow 6a^4 - 7a^3 - 8a^2 > 1 \\ &\Leftrightarrow a^3(4a - 7) + 2a^2(a^2 - 4) > 1, \text{ which is true for } a \geq 2. \end{aligned}$$

Thus for all bigA- $K_3N$ 's  $H < 2a^2$ , and Theorem 4.1 follows.  $\square$

It is easily shown that  $H \leq g(a) < 2a^2$  in case (c) as well as case (b) and, for  $H \geq 6$ ,  $g^{-1}(H) > \sqrt{\frac{H}{2}}$ ; hence for all  $K_3N$ 's

$$(4.5) \quad A \leq 3H - g^{-1}(H),$$

which for  $H \geq 6$  is a slightly stronger but less convenient result than Theorem 4.1.

It is also not onerous to extend the approach of case (a) for finding all  $K_3N$ 's with  $a = 1$ : for  $a = 2$ , again there are none (although  $9801 = 9 \cdot 11 \cdot 99$  obeys the Korselt

divisibility criterion); but for  $a = 3$  there are two, the bigA- $C_3N$   $7 \cdot 23 \cdot 41 = 6601$ , and the bigA- $K_3N$

$$(4.6) \quad n^* = 547 \cdot 575 \cdot 659 = 207271975.$$

Actually from (4.3),  $g(3) = 14$ , giving rise to  $n^*$  with  $(A, B, C) = (39, 41, 47)$  and  $(\alpha, \beta, \gamma) = (-3, -1, 5)$ ; and  $39 = A < 3H - \sqrt{\frac{H}{2}} \simeq 39.35$ .  $n^*$  is the only  $K_3N$  with equality in (4.5), since  $g(5)$  is irrational, and for  $a \geq 7$  we have

$$6a^2 - 10a + 15 < \sqrt{(6a^2 - 10a + 15)^2 + 68a - 44} < 6a^2 - 10a + 16,$$

so from (4.3)  $g(a)$  is irrational. Gordon Davies (see §5.1) did a computer search for bigA- $K_3N$ 's with  $S = 1$ , using  $(\alpha, \beta, \gamma) = (-a, -a + 2t, 2a - 2t + 1)$ , for odd  $a$  up to 1239 and  $1 < t < \frac{3a}{4}$ : no more were found, and  $H^*$  was rational only for  $a = 151$ ,  $t = 89$ , giving  $H^* = 13067\frac{1}{3}$ .

In like manner to (4.4) we find

$$\begin{aligned} H^\dagger(a, S, 0) &= \frac{1}{6S}(4a\sigma - 2\sigma^2 + 9 + \sqrt{4(\sigma^2 + 3)(a + \sigma)^2 + 81}) \\ &= \frac{1}{12S}\{(a + S)(3a - S) + 18 + \sqrt{[(a + S)^2 + 12](3a + S)^2 + 324}\}, \end{aligned}$$

so for fixed  $S$  and large  $a$  we have  $H^\dagger(a, S, 0) \sim \frac{a^2}{2S}$  and  $H^\dagger(a, S, a + \sigma) \sim \frac{2a^2}{S}$ , whence  $(1 + o(1))\frac{a^2}{2S} < H^* < (1 + o(1))\frac{2a^2}{S}$ . Hence with  $\lambda := \frac{a^2}{H}$  and  $A = 3H - \sqrt{\lambda H}$ , for  $a \gg S$  we expect  $\frac{S}{2} < \lambda < 2S$ ; we may regard  $\frac{A}{H} < 3$  and  $\lambda > \frac{1}{2}$  as different measures of closeness to the bound of Theorem 4.1. For  $n < 10^{24}$ , there are only 71 bigA- $C_3N$ 's, and just 11 with  $\frac{A}{H} > 2$ ; the two largest  $\frac{A}{H}$  values are about 2.342 and 2.683, and only these two bigA- $C_3N$ 's have  $a > S$ . With  $\frac{A}{H} \simeq 2.683$ , we have  $n^\dagger := 835327 \cdot 893359 \cdot 1117117 = 833645090806507981$ , with  $(A, B, C, H) = (1497, 1601, 2002, 558)$ , so  $a = 177$ ,  $S = 78$  and  $\lambda \simeq 56.15$ . For  $n^*$ , from (4.6),  $\frac{A}{H} \simeq 2.786$  and  $\lambda = \frac{9}{14}$ . I was able to find marginal improvements on the bound of Theorem 4.1 for sufficiently large  $a$  (e.g. (4.7) below), but none implying  $\lambda > \mu$  for some  $\mu > \frac{1}{2}$ .

Challenges 1(a): Find a bigA- $K_3N$  with  $a > 3$  and  $S = 1$ .

1(b): Find a bigA- $C_3N$  with  $n > 6601$  and  $\lambda < 10$ .

**Theorem 4.2.** For any  $K_3N$ ,  $A < \sqrt{3(p-1)} - \frac{1}{2} \sqrt[4]{\frac{p-1}{12}}$ .

*Proof.* Using the notation and from the above discussion of Theorem 4.1, Theorem 4.2 holds for  $n^*$  and for  $n = 6601$ , and hence for  $a \leq 3$ . For  $S \geq 2$  and  $a \geq 4$ , from (4.4b) we have

$$\begin{aligned} H &< H^\dagger(a, 2, \frac{3a+2}{2}) = \frac{1}{12}(6a^2 + 8a + 9 + \sqrt{4(a^2 + 3)(3a + 2)^2 + 81}) \\ &< \frac{1}{12}(6a^2 + 8a + 9 + \sqrt{4(a + 1)^2(3a + 2)^2}) \\ &= a^2 + \frac{3}{2}a + \frac{13}{12} < 2\left(a - \frac{1}{2}\right)^2 \quad \text{since } a \geq 4; \end{aligned}$$

and for  $S = 1$ ,  $a$  is odd, and for  $a \geq 5$  from (4.3),  $H \leq g(a) < 2(a - \frac{1}{2})^2$ . Hence for  $a \geq 4$ , for any  $K_3N$ ,  $H < 2(a - \frac{1}{2})^2$ , so  $a > \sqrt{\frac{H}{2}} + \frac{1}{2}$  and

$$(4.7) \quad A < 3H - \sqrt{\frac{H}{2}} - \frac{1}{2}$$

Let  $f(x) := \frac{3p'}{x} - x - \sqrt{\frac{p'}{2x}} - \frac{1}{2}$ . Then since  $H = \frac{p'}{A}$ , from (4.7)  $f(A) > 0$ . Also

$$f'(x) = -\frac{3p'}{x^2} - 1 + \frac{1}{2}\sqrt{\frac{p'}{2x^3}} = -\frac{\sqrt{p'}}{2\sqrt{2}x^2}(6\sqrt{2p'} - \sqrt{x}) - 1 < 0 \quad \text{for } 0 < x < p',$$

so  $f(x)$  decreases as  $x$  increases over this interval, which certainly contains  $A$ .

Writing  $\rho := \sqrt[4]{3p'}$  and  $\mu := \sqrt{\rho^2 - \frac{\rho}{2\sqrt{6}}}$  we have

$$\begin{aligned} f\left(\sqrt{3p'} - \frac{1}{2}\sqrt[4]{\frac{p'}{12}}\right) &= f(\mu^2) = \frac{\rho^4}{\mu^2} - \mu^2 - \frac{\rho^2}{\sqrt{6}\mu} - \frac{1}{2} \\ &= \frac{1}{\sqrt{6}\mu^2} \{\sqrt{6}(\rho^4 - \mu^4) - \rho^2\mu\} - \frac{1}{2} = \frac{1}{\sqrt{6}\mu^2} \left(\rho^3 - \frac{\sqrt{6}}{24}\rho^2 - \rho^2\mu\right) - \frac{1}{2} \\ &= \frac{\rho^2 \{(\rho - \frac{\sqrt{6}}{24})^2 - \mu^2\}}{\sqrt{6}\mu^2(\rho - \frac{\sqrt{6}}{24} + \mu)} - \frac{1}{2} = \frac{\rho^2}{96\sqrt{6}\mu^2(\rho + \mu - \frac{\sqrt{6}}{24})} - \frac{1}{2} \end{aligned}$$

But  $p \geq 3$ , so  $\rho > 1.565, \mu > 1.459$ ,  $\frac{\rho^2}{\mu^2} < 1.15$ ,  $\frac{\rho^2}{96\sqrt{6}\mu^2(\rho + \mu - \frac{\sqrt{6}}{24})} < 0.00168$

and  $f(\mu^2) < 0$ , whence since  $f(A) > 0$  and  $f(x)$  decreases with  $x$ ,  $A < \mu^2$ , giving Theorem 4.2.  $\square$

For  $n^*$  (see (4.6)),  $A = 39 < \sqrt{3p'} - \frac{1}{2}\sqrt[4]{\frac{p'}{12}} \simeq 39.1736$ .

In seeking an upper bound for  $B$  given  $p$ , we know from Theorem 3.1 that we can have  $q' = p'(2p - \sqrt{p - \frac{3}{4}} + \frac{1}{2})$ , with  $H = p'$  and  $B = 2p - \sqrt{p - \frac{3}{4}} + \frac{1}{2}$ ; we show that it is possible for  $B$  marginally to exceed this:

**Theorem 4.3.** (a) For any  $K_3N$ ,  $B < 2p - \sqrt{p - \frac{3}{4}} + \frac{\sqrt{3}+1}{2\sqrt{3}}$   
 (b) For any  $C_3N$ ,  $B < 2p - \sqrt{p - \frac{3}{4}} + \frac{\sqrt{7}+1}{2\sqrt{7}}$

*Proof.* Write  $S = \sqrt{p - \frac{3}{4}} - \frac{1}{2}$ . We seek  $B > 2p - S$ , and we consider two cases:

(i)  $G \geq 2$ . Then from Theorem 2.2,  $E \leq p - 1$ , and from (2.19)

$$B = \frac{p+E}{G} \leq \frac{2p-1}{2} < p < 2p - S$$

(ii)  $G = 1$ . Then from (2.19)  $B = p + E$  and from (2.10)  $E = p - s$ , so

$$(4.8) \quad B = 2p - s$$

Also from (2.20),  $\Delta = AG = A$ , whence from (2.11)

$$(4.9) \quad \eta = \frac{s^2 + A}{p - s}$$



and using (2.9b) and (2.10),  $CH = r' = \frac{AH(p+D)}{A}$ , so

$$(4.10) \quad C = p + D = 2p + s + \eta$$

Since  $H$  is even, from (2.18)

$$(4.11) \quad H = AF - 1 \quad \text{and } A \text{ and } F \text{ are both odd, and also}$$

$$(4.12) \quad p = AH + 1 = FA^2 - A + 1.$$

We now consider the two sub-cases (a)  $\eta \geq 2$  and (b)  $\eta = 1$ .

(a) If  $\eta \geq 2$ , from (4.9) we have  $s^2 + A \geq 2(p - s)$ , whence  $s^2 + 2s \geq 2p - A$  and  $s \geq \sqrt{2p - A + 1} - 1 > \sqrt{2p - \sqrt{3p - 3} + 1} - 1$ , using Theorem 4.2.

But  $\sqrt{2p - \sqrt{3p'} + 1} - 1 > S$  reduces to  $p + \frac{3}{2} > \sqrt{p - \frac{3}{4}} + \sqrt{3p'}$ , which is true for  $p \geq 3$ , so  $s > S$  and from (4.8)  $B < 2p - S$ .

(b) If  $\eta = 1$ , from (4.9)  $s^2 + A = p - s$ , whence from (4.12)

$$(4.13a) \quad s^2 + s = s(s + 1) = FA^2 - 2A + 1 = F'A^2 + A'^2 \quad \text{and}$$

$$(4.13b) \quad s = \sqrt{FA^2 - 2A + \frac{5}{4}} - \frac{1}{2}$$

From (4.13a) we note that  $F = 1$  implies  $A'^2 = s(s + 1)$ , which is impossible. So by (4.11) for odd  $F \geq 3$ , remembering that  $x = x' + 1$  and using (4.12) again, we have

$$S - s = \sqrt{FA^2 - A + \frac{1}{4}} - \sqrt{FA^2 - 2A + \frac{5}{4}} = \frac{A'}{\sqrt{(F'A^2 + (A - \frac{1}{2})^2) + \sqrt{F'A^2 + A'^2 + \frac{1}{4}}}}$$

Hence if  $A = 1$ ,  $s = S$  as for Theorem 3.1, but if  $A \geq 3$  ( $A$  is odd by (4.11)) then

$$S - s = \frac{1}{\sqrt{F'(1 + \frac{1}{A'})^2 + (1 + \frac{1}{2A'})^2} + \sqrt{F'(1 + \frac{1}{A'})^2 + 1 + \frac{1}{4A'^2}}} > 0$$

From this we deduce that  $0 < S - s < \frac{1}{2\sqrt{F}} \leq \frac{1}{2\sqrt{3}}$  since  $F \geq 3$ ,

whence  $2p - S < B = 2p - s < 2p - S + \frac{1}{2\sqrt{3}}$ , giving Theorem 4.3(a).

Also we see that for given  $F$ , if there is an infinite sequence of  $K_3N$ 's with increasing  $A$  values, then  $2p - S + \frac{1}{2\sqrt{F}} - B \rightarrow 0+$  as  $A \rightarrow \infty$ . There is such a sequence iff (4.13a) has an infinite number of solutions for  $s$  and  $A$  which result in pairwise coprime  $A$ ,  $B$  and  $C$ , and  $E \geq 2$ . Such solutions we call *acceptable*. With

$$(4.14) \quad \phi := 2FA - 2 = 2H, \quad \theta = 2s + 1, \quad (4.13a) \text{ implies}$$

$$(4.15) \quad \phi^2 - F\theta^2 = 4 - 5F,$$

and from the theory of quadratic forms a necessary condition for this to have a solution is that  $x^2 \equiv F \pmod{(5F - 4)}$  be soluble.

If  $F \equiv 0 \pmod{3}$ , suppose  $(\phi, \theta)$  gives an acceptable solution. Then *working in*  $\mathbb{Z}_3$ , from (4.14)  $\theta = 2s + 1$ , so  $s = 2\theta + 1$ , from (4.13a)  $s(s + 1) = FA^2 - 2A + 1$ , so  $A = (2\theta + 1)(2\theta + 2) - 1 = \theta^2 + 1$ , from (4.11)  $H = FA - 1 = 2$ ; so  $p = AH + 1 = 2\theta^2 + 2$  unless  $\theta = 0$ ,  $p = 0$ ; from (4.8)  $B = 2p - s = \theta^2 - 2\theta - 1 = (\theta - 1)^2 + 1$ , so  $q = BH + 1 = 2(\theta - 1)^2 + 2$  unless  $\theta = 1$ ,  $q = 0$ ; with  $\eta = 1$ , from (4.8, 4.10, 4.14)  $C = B + \theta = \theta^2 - \theta + 2$ , so  $r = CH + 1 = 2\theta(\theta - 1) + 2 = 2$  unless  $\theta = 2$ ,  $r = 0$ .

Thus in  $\mathbb{Z}_3$ , for any  $\theta$  exactly one of  $p, q, r$  is zero, whence in  $\mathbb{Z}$   $3|p, q$  or  $r$  and so  $n$  is only a  $C_3N$ , possibly, if  $p = 3$ , in which case  $n = 561$ , with  $A = 1$ .

For  $F = 5$ , (4.15) is  $\phi^2 - 5\theta^2 = -21$ , but  $x^2 \equiv 5 \pmod{21}$  has no solutions, so neither has (4.15). Thus there are no  $C_3N$ 's with  $A > G = \eta = 1$  and  $F < 7$ , and Theorem 4.3(b) follows in like manner to Theorem 4.3(a) above.  $\square$

From (4.14) for a solution to (4.15) to yield a solution to (4.13a) we need  $\phi \equiv -2 \pmod{2F}$  and  $\theta$  odd. Clearly from (2.10) and (4.9) with  $\eta = 1$ ,  $E = p - s = s^2 + A \geq 2$ , as required. Also such a solution will result in positive integers  $A, B, C, H, F$  which satisfy (2.5a), whence we have  $h := \gcd(A, B, C) = \gcd(A, B) = \gcd(A, C) = \gcd(B, C)$ ; and from (4.8) and (4.12)  $s \equiv 2 \pmod{h}$ , whence from (4.13a)  $6 \equiv 1 \pmod{h}$ , so  $h = 1$  or  $5$ . Then if  $h = 5$ , from (4.14) we have  $(\phi, \theta) \equiv (3, 0) \pmod{5}$ ; so if  $(\phi, \theta) \not\equiv (3, 0) \pmod{5}$  then  $h = 1$  and our solution is acceptable.

Using the theory of Pell's equation, if  $\phi_i^2 - F\theta_i^2 = k$ ,  $x^2 - Fy^2 = 1$  and

$$(4.16) \quad \phi_{i+1} = (2Fy^2 + 1)\phi_i + 2Fxy\theta_i, \quad \theta_{i+1} = 2xy\phi_i + (2Fy^2 + 1)\theta_i,$$

then  $\phi_{i+1}^2 - F\theta_{i+1}^2 = k$  and  $\phi_{i+1} \equiv \phi_i \pmod{2F}$ ; so (4.15) has an infinite sequence of acceptable solutions if it has a solution  $(\phi_1, \theta_1)$  with  $\phi_1 \equiv -2 \pmod{2F}$  (unless, if possible,  $(\phi_1, \theta_1) \equiv (3, 0)$  and  $y \equiv 0 \pmod{5}$ ). If  $F = s^2 + s + 1$ , as for the  $K_3$ -family  $\{n_2(s)\}$  (equations (3.4)) then  $(\phi_1, \theta_1) = (2s(s+1), 2s+1)$  is acceptable and gives rise to  $n_2(s)$  with  $A = 1$  and  $B = 2p - S$ . Also there are acceptable solutions with  $F \neq s^2 + s + 1$ : for example for  $F = 87$ ,  $(\phi_1, \theta_1) = (1912, 205)$  and  $A = 11$ .

For  $F = 3$ ,  $s = 1$ , so  $(\phi_1, \theta_1) = (4, 3)$ , which gives  $n_2(1) = 561$ ; and for  $F = 7$ ,  $s = 2$ ,  $(\phi_1, \theta_1) = (12, 5)$ , (4.16) is  $\phi_{i+1} = 127\phi_i + 336\theta_i$ ,  $\theta_{i+1} = 48\phi_i + 127\theta_i$ , and  $(\phi_2, \theta_2) = (3204, 1211)$  leads via (4.14, 4.11, 4.8, 4.10) to  $A = 229$ ,  $s = 605$ ,  $H = 1602$ ,  $p = 366859$ ,  $B = 733113$ ,  $q = 1174447027$ ,  $C = 734324$ ,  $r = 1176387049$  and  $2p - S \simeq 733112.8118 < B = 733113 < 2p - S + \frac{1}{2\sqrt{7}} \simeq 733113.000737$  for the  $K_3N$   $n = pqr$ .

If  $n(i)$  is the  $K_3N$  arising from  $(\phi_i, \theta_i)$  for  $F = 7$ , it is easily shown that, for  $i \geq 2$ ,  $n(i+1) \simeq 254^8 n(i) \simeq 1.73 \times 10^{19} n(i)$ , and a naive "probability" estimate based on the knowledge that  $n(2)$  is not a  $C_3N$  and an assumption of the independence of the primality of  $p, q$  and  $r$  is: " $p$ "( $n(i)$  is a  $C_3N$  for some  $i > 2$ )  $\simeq \frac{1}{2000}$ .

Challenges 2(a): Find a  $C_3N$  with  $B > 2p - \sqrt{p - \frac{3}{4}} + \frac{1}{2} + \frac{1}{4\sqrt{3}}$ .

2(b): Find a  $C_3N$  with  $B > 2p - \sqrt{p - \frac{3}{4}} + \frac{1}{2}$ .

From Theorem 3.2,  $r' = \frac{1}{2}p'(p+1)^2$  is possible, so given  $p$  we can have  $C = \frac{1}{2}(p+1)^2$ . Again, we show that this can be slightly exceeded:

**Theorem 4.4.** *For any  $K_3N$ ,  $C \leq \frac{1}{2}(p^2 + 2p + \frac{1}{2}\sqrt{4p-3} + \frac{1}{2})$ , with equality iff  $E = 2$ ,  $F = G = 1$ .*

*Proof.* For any  $K_3N$ ,  $A < p$ , and so from (2.16) and (2.19) we have

$$(4.17) \quad C = \frac{p^2}{EG} + \frac{p}{G} + \frac{A}{E} < \frac{p^2}{EG} + \frac{p}{G} + \frac{p}{E}$$

But  $E \geq 2$  and  $G \geq 1$ , so if  $E \geq 3$  then  $C < \frac{p^2}{3} + p + \frac{p}{3} = \frac{p(p+4)}{3} < \frac{1}{2}(p+1)^2$  for  $p \geq 3$ , and if  $G \geq 2$  then  $C < \frac{p^2}{4} + \frac{p}{2} + \frac{p}{2} = \frac{p(p+4)}{4} < \frac{1}{2}(p+1)^2$ ; thus  $C < \frac{1}{2}(p+1)^2$

unless  $E = 2, G = 1$  in which case, since  $G = 1$ , from (4.12)  $FA^2 - A - p' = 0$ ,

whence  $A = \frac{1 + \sqrt{4Fp' + 1}}{2F} = \frac{1}{2F} + \frac{1}{2\sqrt{F}}\sqrt{4p' + \frac{1}{F}} \leq \frac{1}{2}(1 + \sqrt{4p - 3})$ , with equality

iff  $F = 1$ . Hence from (4.17),  $C \leq \frac{p^2}{2} + p + \frac{1}{4}(1 + \sqrt{4p - 3})$ , and Theorem 4.4 follows.  $\square$

For a  $K_3$ -family with equality in Theorem 4.4, from (2.18), (2.19) and (2.16) we get

$$(4.18) \quad A = A(H) := H + 1, \quad B = AH + 3 = B(H) := H^2 + H + 3, \\ C = C(H) := \frac{1}{2}(H^4 + 2H^3 + 5H^2 + 5H + 4)$$

$$p = P(H) := H^2 + H + 1, \quad q = Q(H) := H^3 + H^2 + 3H + 1,$$

$$r = R(H) := \frac{1}{2}(H^5 + 2H^4 + 5H^3 + 5H^2 + 4H + 2) \quad \text{and}$$

(4.19)

$$n = N(H) := \frac{1}{2}(H^{10} + 4H^9 + 14H^8 + 30H^7 + 53H^6 + 69H^5 + 71H^4 + 55H^3 + 31H^2 + 12H + 2)$$

With  $H = 2h$  this yields a  $K_3$ -family with parameter  $h$ , but from (4.18) if  $H \equiv 2 \pmod{3}$  then  $\gcd(A, B) = 3$ , so we take  $H = 6t$  or  $H = 6t + 4$  to get two  $K_3$ -families with the required maximal  $C$  property. Also if  $H \equiv 1 \pmod{3}$  then  $3|p$  and  $3|q$ , so for  $C_3N$ 's we must have the  $K_3$ -family with  $H = 6t$ . A search by Matthew Williams (see §5.1) up to  $t = 1365$  found  $C_3N$ 's only for  $t = 1$  and  $t = 210$ , giving  $n = 43 \cdot 271 \cdot 5827 = 67902031$ , with  $A = 7, B = 45, C = 971$ , and  $n = 1588861 \cdot 2001967381 \cdot 1590423947471521 = 5058896665381789187674264635361$ , with  $A = 1261, B = 1588863, C = 1262241228152$ .

The above  $K_3$ -families will be shown to exemplify further bounds in Theorems 4.9 and 4.10.

#### 4.2. An upper bound for $q$ , given $p$ and $n$ .

**Theorem 4.5.** *For any  $K_3N$ ,  $q < \sqrt{\frac{n}{p}} - \sqrt{\frac{p}{12}}$ .*

*Proof.* Since  $r \geq q + H$ , we have  $q = \frac{n}{pr} \leq \frac{n}{p(q + H)}$ , whence  $pq^2 + pHq - n \leq 0$

$$\text{and } q \leq \sqrt{\frac{n}{p} + \frac{H^2}{4}} - \frac{H}{2}. \quad \text{Now } \sqrt{\frac{n}{p} + \frac{H^2}{4}} - \frac{H}{2} < \sqrt{\frac{n}{p}} - \sqrt{\frac{p}{12}}$$

$$\text{iff } \sqrt{\frac{n}{p} + \frac{H^2}{4}} - \sqrt{\frac{n}{p}} < \frac{H}{2} - \sqrt{\frac{p}{12}} = \frac{1}{2}\left(H - \sqrt{\frac{AH + 1}{3}}\right);$$

$$\text{also } \sqrt{\frac{n}{p} + \frac{H^2}{4}} - \sqrt{\frac{n}{p}} = \frac{H^2}{4(\sqrt{qr} + \frac{H^2}{4} + \sqrt{qr})} < \frac{H^2}{8\sqrt{qr}} < \frac{H^2}{8\sqrt{q'r'}} = \frac{H}{8\sqrt{BC}},$$

so Theorem 4.5 follows if we can show that  $\frac{H}{8\sqrt{BC}} < \frac{1}{2}\left(H - \sqrt{\frac{AH + 1}{3}}\right)$ , i.e.

$$(4.20) \quad 1 < 4\sqrt{BC}\left(1 - \sqrt{\frac{A}{3H} + \frac{1}{3H^2}}\right).$$

We consider two cases: (i) if  $\frac{A}{H} < \frac{13}{6}$ , then since  $B \geq 2, C \geq 3$  and  $H \geq 2$ ,

$$\left(1 - \frac{1}{4\sqrt{BC}}\right)^2 - \frac{1}{3H^2} \geq \left(1 - \frac{1}{4\sqrt{6}}\right)^2 - \frac{1}{12} > \frac{13}{18} > \frac{A}{3H}, \quad \text{whence (4.20) follows.}$$

(ii) If  $\frac{A}{H} \geq \frac{13}{6}$ , then  $n$  is a big  $A$ - $K_3N$ ,  $B > A \geq \frac{13H}{6}$  and  $C = 3H + \gamma > 3H$  (since  $\gamma > 0$ , see the proof of Theorem 4.1, just after (4.1)). From Theorem 4.1,

$$A < 3H - \sqrt{\frac{H}{2}}, \quad \text{so} \quad \frac{A}{3H} + \frac{1}{3H^2} < 1 - \frac{1}{3\sqrt{2H}} + \frac{1}{3H^2}. \quad \text{Now} \quad 1 - (1-x)^{\frac{1}{2}} > \frac{1}{2}x$$

$$\begin{aligned} \text{for } 0 < x < 1. \text{ Hence } 4\sqrt{BC}\left(1 - \sqrt{\frac{A}{3H} + \frac{1}{3H^2}}\right) &> 4\sqrt{BC}\left\{1 - \left[1 - \left(\frac{1}{3\sqrt{2H}} - \frac{1}{3H^2}\right)\right]^{\frac{1}{2}}\right\} \\ &> 4\sqrt{\left(\frac{13H}{6}\right) \cdot 3H}\left\{\frac{1}{2}\left(\frac{1}{3\sqrt{2H}} - \frac{1}{3H^2}\right)\right\} = \frac{\sqrt{26}}{3}\left(\sqrt{\frac{H}{2}} - \frac{1}{H}\right) > 1 \quad \text{for } H \geq 4, \end{aligned}$$

which is (4.20); and for  $H = 2$ , since  $\frac{13H}{6} \leq A < 3H - \sqrt{\frac{H}{2}}$ , we have  $4\frac{1}{3} \leq A < 5$ , which is impossible, establishing the result.  $\square$

For the  $C_3N$   $191 \cdot 421 \cdot 431$ , Theorem 4.5 gives  $q = 421 < 421.981 \simeq \sqrt{\frac{n}{p}} - \sqrt{\frac{p}{12}}$ .

**4.3. Upper bounds given  $n$  for  $p, A, B, C$  and  $ABC$ .** A cursory glance at a list of  $C_3N$ 's suggests that a substantially better bound than the  $p < \sqrt[3]{n}$  given by Theorem 3.4 should be attainable. That this is not so can be seen by considering the Chernick type  $K_3$ -families discussed in §2.2 with  $(A, B, C) = (2u - 1, 2u, 2u + 1)$ . For this family  $\sum A = 6u$ ,  $\sum AB = 12u^2 - 1$ ,  $ABC = 2u(4u^2 - 1)$ , so (2.5a) requires  $H$  and  $F$  satisfying  $(12u^2 - 1)H + 6u = 2u(4u^2 - 1)F$ . We see that for  $u > 1$ ,  $F = 6u^2 - 5$  and  $H = H_o = 4u(u^2 - 1)$  is the unique solution with  $0 < H_o < ABC$ , so the general solution is

$$(4.21) \quad H = H_o + tABC = 2u\{2(u^2 - 1) + (4u^2 - 1)t\} = \frac{B}{2}\{B^2 - 4 + 2(B^2 - 1)t\}.$$

In terms of  $B = 2u$ , this gives

$$\begin{aligned} p_f &:= p_f(u, t) := \frac{1}{2}B(B - 1)\{B^2 - 4 + 2(B^2 - 1)t\} + 1, \\ q_f &:= q_f(u, t) := \frac{1}{2}B^2\{B^2 - 4 + 2(B^2 - 1)t\} + 1, \\ r_f &:= r_f(u, t) := \frac{1}{2}B(B + 1)\{B^2 - 4 + 2(B^2 - 1)t\} + 1, \end{aligned}$$

and we have the two parameter system of  $K_3$ -families  $n_f(u, t) := p_f q_f r_f$  for  $u = 1, t \geq 1$  and  $u > 1, t \geq 0$ . If now we arbitrarily describe any  $KN$  with  $\frac{r}{p} < 1.5$  as “flat”, then  $n_f(u, t)$  gives flat  $K_3N$ 's for  $u \geq 3$ , since in general  $\frac{r}{p} = \frac{CH+1}{AH+1} = \frac{C}{A} - \frac{C-A}{Ap} < \frac{C}{A}$ , giving  $\frac{r}{p} = 1 + \frac{2}{B-1} - \frac{2}{(B-1)p} < 1.4$  for  $B \geq 6$ ; this also shows that for any Chernick type  $K_3$ -family the first member is the “flattest”, since “steepness”  $:= \frac{r}{p}$  increases with  $p$  (and hence  $t$ ). In [12] Pinch says that for  $CN$ 's up to  $10^{15}$  the largest value of  $p$  occurring is 72931, dividing  $651693055693681 = 72931 \cdot 87517 \cdot 102103$ ; this is  $n_f(3, 69)$ . Gordon Davies did a cursory computer search which found the  $C_3N$ 's  $n_f(5, 3), n_f(8, 0), n_f(17, 1), n_f(51, 0)$  and the very flat  $n_f(102, 0) = 861618073 \cdot 865862497 \cdot 870106921 = 649136982888522736355512801$ ,

with “steepness”  $\simeq 1.00985$ . Clearly any improvement on  $p < \sqrt[3]{n}$  will be of the form  $p < (1 - o(1))\sqrt[3]{n}$ , with  $o(1) > 0$ , and we now show that

**Theorem 4.6.** *For any  $K_3N$ ,*

$$p \leq \left\lceil \sqrt[3]{n} - \frac{4\sqrt{3}}{9}\sqrt[6]{n} \right\rceil.$$

*Proof.* If  $k := B - A$  and  $l := C - A$ , for any  $K_3N$  we have  $n = p(p + kH)(p + lH)$ . From Theorem 4.1,  $A < 3H - 1$  so

$$(4.22) \quad H^2 > \frac{AH + H}{3} > \frac{AH + 1}{3} = \frac{p}{3},$$

and hence  $kH \geq H > \sqrt{\frac{p}{3}}$  and for  $l \geq 3$ ,  $lH > 3\sqrt{\frac{p}{3}}$ , while if  $l = 2$  we have  $n \in \{n_f(u, t)\}$ , and  $lH = 2H > 3\sqrt{\frac{p}{3}}$  is equivalent to  $4H^2 > 3p = 3AH + 3$ , i.e. to  $H\{4H - 3(B - 1)\} > 3$ , which is obvious from (4.21); so in all cases  $lH > 3\sqrt{\frac{p}{3}} = \sqrt{3p}$ . So for any  $K_3N$ ,  $n > p(p + \sqrt{\frac{p}{3}})(p + \sqrt{3p})$ , and if  $n = V(V + \sqrt{\frac{V}{3}})(V + \sqrt{3V})$ , then  $p < V$ . Using the approach of Theorem 3.5 to express  $V$  in terms of  $n$  as a power series, if we put  $n = 27y^6$ ,  $V = 3v^2$ ,  $v = y + \sum_{i=0}^{\infty} a_i y^{-i}$  and equate coefficients of  $y^5$ ,  $y^4$  and  $y^3$ , we get  $a_0 = -\frac{2}{9}$ ,  $a_1 = \frac{11}{162}$ ,  $a_2 = -\frac{52}{2187}$  and  $V = 3y^2 - \frac{4}{3}y + \frac{5}{9} - \frac{170}{729y} + \dots$ , whence  $V = \sqrt[3]{n} - \frac{4\sqrt{3}}{9}\sqrt[6]{n} + \frac{5}{9} - \frac{170\sqrt{3}}{729\sqrt[6]{n}} + \dots$ . But  $p < V$  and  $p$  is an integer, so Theorem 4.6 follows.  $\square$

From (4.6) for  $n^*$  we get  $p = 547 < \lceil \sqrt[3]{n} - \frac{4\sqrt{3}}{9}\sqrt[6]{n} \rceil = 574$ , and clearly a marginally lower bound than that given by Theorem 4.6 could readily be established. I speculate that for large  $n$  there is an upper bound  $\sqrt[3]{n} - \mu\sqrt[4]{n}(1 + o(1))$  for some  $\mu > 0$ ; such a bound can be established for the system  $n_f(u, t)$  with  $\mu = \frac{1}{\sqrt[3]{2}}$ . But  $n^*$  (see (4.6)) is both slightly flatter and much smaller than  $n_f(5, 0)$ : if (using the notation of the proof of Theorem 4.1) there were an infinite system of big  $A$ - $K_3N$ 's with  $(\alpha, \beta, \gamma) = (-\sqrt{\frac{H}{2}}, 1, \sqrt{\frac{H}{2}})$ , from (2.6) we can deduce that it would require  $\mu = \frac{1}{\sqrt[3]{108}}$ , suggesting a conjectural upper bound as in Challenge 3 below. But possibly there lurk yet flatter  $K_3N$ 's capable of defeating any  $\mu > 0$ .

Challenge 3: Find a  $K_3N$  with  $p > \lfloor \sqrt[3]{n} - \sqrt[4]{\frac{n}{108}} - \frac{5}{18}\sqrt[6]{\frac{n}{27}} + \frac{5}{72}\sqrt[12]{\frac{n}{216}} \rfloor$ , or prove that none exists.

**Theorem 4.7.** *For any  $K_3N$ ,*

$$A < \sqrt{3}\sqrt[6]{n} - \frac{1}{2\sqrt[4]{12}}\sqrt[12]{n}$$

*Proof.* From Theorem 4.2,  $A < \sqrt{3p} - \frac{1}{2}\sqrt[4]{\frac{p}{12}}$ , and from Theorem 4.6 we have  $p < \sqrt[3]{n} - \frac{4\sqrt{3}}{9}\sqrt[6]{n} + 1 < \sqrt[3]{n}$ , giving the result at once.  $\square$

Clearly a slightly tighter bound could easily be found. For  $n^*$  (see 4.6) this gives  $A = 39 < \sqrt{3}\sqrt[6]{n} - \frac{1}{2\sqrt[4]{12}}\sqrt[12]{n} \simeq 40.81$ .

If  $B^\dagger(n)$  is to be a bound for all  $K_3N$ 's for  $B$  given  $n$  for which  $\inf(B^\dagger(n) - B) = 0$ , then  $B^\dagger(n)$  as in Theorem 4.8 (a) below suffices. But if we are content with  $\inf(\frac{B^\dagger(n)}{B}) = 1$  then we could much more easily establish  $B^\dagger(n) = \sqrt{2}\sqrt[4]{n}$ . However, we outline a proof of

**Theorem 4.8.** (a) For any  $K_3N$ ,  $B < \sqrt{2}\sqrt[4]{n} - \left(\sqrt{3} - \frac{1}{2}\right)\sqrt[8]{\frac{n}{4}} + \frac{39 + \sqrt{3}}{24}$   
 (b) For any  $C_3N$  except 6601,  $B < \sqrt{2}\sqrt[4]{n} - \left(\sqrt{7} - \frac{1}{2}\right)\sqrt[8]{\frac{n}{4}} + \frac{175 - 3\sqrt{7}}{56}$

*Proof.* We define  $B_\mu(n) := \sqrt{2}\sqrt[4]{n} - \left(\sqrt{\mu} - \frac{1}{2}\right)\sqrt[8]{\frac{n}{4}} + \frac{3\mu^2 - \mu\sqrt{\mu} + 4\mu + 4\sqrt{\mu}}{8\mu}$ , and then (a) states  $B < B_3(n)$  and (b) states  $B < B_7(n)$ . Also for any  $KN$ ,  $n \geq 561$ , and so  $B_7(n) < B_3(n)$ . Further, if we put  $u = \sqrt[8]{\frac{n}{4}}$ , we have

$$(4.23) \quad B_\mu(n) = B_\mu^*(u) := 2u^2 - \left(\sqrt{\mu} - \frac{1}{2}\right)u + \frac{3\mu + 4}{8} - \frac{\mu - 4}{8\sqrt{\mu}}$$

We note that for  $\mu \leq 7$ ,  $B_\mu$  and  $B_\mu^*$  are increasing functions for  $n \geq 561$  (actually, for  $\mu \leq 62.7$ ).

We consider three cases: (i)  $G \geq 2$ , (ii)  $G = 1, F \geq 2$  and (iii)  $G = F = 1$ .

(i) For  $G \geq 2$ , from Theorem 2.2 and (2.19),  $B < p$ . Also from (4.22)  $H^2 > \frac{p}{3}$ , so  $p'(H^2 + F) > p'(\frac{p}{3} + 1) = \frac{p^2 + 2p - 3}{3} > \frac{p^2}{3}$  for  $p \geq 3$ . Hence, with (2.6) and since  $C > B$ , we have  $n > n' = ABCH(H^2 + F) > B^2p'(H^2 + F) > \frac{B^2p^2}{3} > \frac{B^4}{3}$ , so  $B < \sqrt[4]{3n}$ . This immediately gives  $B < \sqrt{2}\sqrt[4]{n}$ , but the tighter bound  $B_7(n)$  then requires  $\sqrt[4]{3n} < B_7(n)$ , which holds for  $n > 5.625 \times 10^9$ ; a computer check verified Theorem 4.8 for  $n < 5.625 \times 10^9$ .

(ii) For  $G = 1$  from (4.11)  $F$  is odd, so  $F \geq 3$ , and  $H = AF - 1$ , so  $H^2 = Fp' - H$ . Also  $\eta \geq 1$  and from (2.20)  $\frac{p'}{\Delta} = \frac{AH}{AG} = H \leq p'$ . Hence, and from (2.15), we get

$$\begin{aligned} n &= p\{H^2(4p^2 + \eta p) + H(5p + \eta - 1) + 1\} \geq p\{H^2(4p^2 + p) + 5Hp + 1\} \\ &= p\{(Fp' - H)(4p^2 + p) + 5pH + 1\} = p\{Fpp'(4p + 1) - 4pp'H + 1\} \\ &\geq p\{3pp'(4p + 1) - 4pp'^2 + 1\} = 8p^4 - p^3 - 7p^2 + p \end{aligned}$$

So if we put  $w := w(p) := \sqrt[8]{\frac{1}{4}(8p^4 - p^3 - 7p^2 + p)}$  we have  $w \leq u = \sqrt[8]{\frac{n}{4}}$ , and with  $\mu = 7$  in (4.23) we get  $B_7^*(w) \leq B_7^*(u) = B_7(n)$  for  $p \geq 3$ . Also from Theorem 4.3 we have  $B < B(p) := 2p - \sqrt{p - \frac{3}{4}} + \frac{\sqrt{3} + 1}{2\sqrt{3}}$ . We now want  $B(p) < B_7^*(w)$  for  $p \geq 3$ , i.e.  $\beta(p) := B_7^*(w(p)) - B(p) > 0$ . The dominant term in  $\beta(p)$  is  $2(\sqrt[4]{2} - 1)p$ , so  $\beta(p) > 0$  for sufficiently large  $p$ , and  $\beta(3) \simeq 0.596 > 0$ ; an outline of a general proof is as follows: using the substitution  $p = p(v) := v^2 + v + 1$ , we get from  $w(p)$  above

$$(4.24) \quad \begin{aligned} w &= w^\dagger(v) := w(p(v)) \\ &= \sqrt[8]{\frac{1}{4}(8v^8 + 32v^7 + 79v^6 + 125v^5 + 139v^4 + 107v^3 + 54v^2 + 16v + 1)} \end{aligned}$$

and also  $B_7^\dagger(v) := B_7^*(w^\dagger(v))$ ,  $B_m := B_m(v) := 2p(v) - \sqrt{p(v) - \frac{3}{4}} + \frac{1}{2} = 2v^2 + v + 2$ , and then

$$(4.25) \quad \begin{aligned} \beta^\dagger(v) &:= \beta(p(v)) = B_7^\dagger(v) - B_m(v) - \frac{1}{2\sqrt{3}} \\ &= 2w^2 - B_m - \left(\sqrt{7} - \frac{1}{2}\right)w + \frac{175 - 3\sqrt{7}}{56} - \frac{1}{2\sqrt{3}} \end{aligned}$$

**Lemma 4A.** *If  $x > 0$ ,  $y > 0$  and  $x^4 > y^4$ , then  $x > y$  and*

$$x - y = \frac{x^4 - y^4}{x^3 + x^2y + xy^2 + y^3} > \frac{x^4 - y^4}{4x^3}$$

Applying this Lemma in (4.25) to  $2w^2 - B_m$ , with (4.24) we get

$$\begin{aligned} 2w^2 - B_m &> \frac{16w^8 - B_m^4}{4 \cdot 8w^6} \\ &= \frac{16v^8 + 96v^7 + 228v^6 + 396v^5 + 411v^4 + 324v^3 + 128v^2 + 32v - 12}{4(32v^8 + 128v^7 + 316v^6 + 500v^5 + 556v^4 + 428v^3 + 216v^2 + 64v + 4)^{\frac{3}{4}}} \end{aligned}$$

Now for  $v \geq 10$  we have  $50v^8 > 16(w^\dagger(v))^8$ , so

$$2w^2 - B_m > \frac{4v^8 + 24v^7 + 57v^6}{50^{\frac{3}{4}}v^6} > \frac{1}{5} \left( v^2 + 6v + \frac{57}{4} \right),$$

and hence from (4.25)

$$\begin{aligned} \beta^\dagger(v) &> \frac{1}{5} \left( v^2 + 6v + \frac{57}{4} \right) - \left( \sqrt{7} - \frac{1}{2} \right) w^\dagger(v) > \frac{4v^2 + 24v + 57}{20} - \left( \sqrt{7} - \frac{1}{2} \right) \sqrt[8]{\frac{50}{16}} v \\ &> \frac{4v^2 + 24v + 57}{20} - \frac{5}{2}v = \frac{4v^2 - 26v + 57}{20} > 0 \quad \text{for } v \geq 10 \end{aligned}$$

For  $v = 10$ ,  $p = 111$ , and a computer check verified Theorem 4.8 for all  $K_3N$ 's with  $3 \leq p \leq 109$ .

(iii) Let  $n_o$  be a  $K_3N$  with associated  $K$ -variables  $H_o, A_o, p_o$ , etc, with  $F_o = G_o = 1$ . Then from (2.18)  $A_o = H_o + 1$ , so  $p_o = H_o^2 + H_o + 1$ , from (2.20)  $\Delta_o = A_o G_o = H_o + 1$ , from (2.14a)  $B_o = 2p_o + \frac{\eta_o - \theta_o}{2}$ , and  $\Delta_o < P_o$ , so the conditions needed for the proof of Theorem 3.1 and case (ii) of Theorem 3.5 are met, and in a similar manner we define real variables  $n, p, A, B$  etc in terms of independent real variables  $H$  and  $\eta$ . Then, keeping  $H = H_o$ , constant, we get from the above with (2.13a), (2.14a) and (2.15)

$$(4.26) \quad B = B(H, \eta) := 2H^2 + 2H + 2 + \frac{1}{2}(\eta - \sqrt{4\eta H^2 + 4\eta'(H+1) + \eta^2})$$

and

$$(4.27) \quad \begin{aligned} n = n(H, \eta) &:= 4H^8 + 12H^7 + (24 + \eta)H^6 + (33 + 2\eta)H^5 + (34 + 3\eta)H^4 \\ &\quad + (26 + 3\eta)H^3 + (14 + 2\eta)H^2 + (5 + \eta)H + 1 \end{aligned}$$

Then as for Theorems 3.1 and 3.5 we have that as  $\eta$  increases, so  $B$  decreases and  $n$  increases, so if  $1 \leq \eta_a \leq \eta_o$ , then  $B(H_o, \eta_o) \leq B(H_o, \eta_a)$  and  $n(H_o, \eta_o) \geq n(H_o, \eta_a)$ . So for the best possible bound we want to choose  $\eta_a$  to be the smallest possible  $\eta_o$  (we already know from the proof of Theorem 4.3 that  $\eta_o = 1 = F_o = G_o$  is impossible for  $K_3N$ 's). Dropping the zero suffixes for our  $K_3N$ , from (2.12) we have  $s^2 + \eta s = \eta(H^2 + H + 1) - (H + 1) = \eta H^2 + \eta' H + \eta'$  and with (2.13b) we get

$$(4.28) \quad \phi := 2\eta H + \eta - 1 \quad \text{and} \quad \theta = 2s + \eta \quad \text{and then}$$

$$(4.29) \quad \phi^2 - \eta\theta^2 = -(\eta^3 + 3\eta^2 - 2\eta - 1)$$

Compare this with (4.14) and (4.15) and the accompanying discussion of Pellian solutions, which we now apply to (4.28) and (4.29). We define *acceptable* solutions to (4.29) in the same way as for (4.15), and for a solution to be *admissible* we require

$\theta - \eta$  even, and  $\phi \equiv \eta - 1 \pmod{4\eta}$  since in (4.28) we have  $H$  even. Henceforth replacing  $F$  with  $\eta$  in (4.16) with  $x^2 - \eta y^2 = 1$ , if  $\eta$  is not a perfect square and (4.29) has a solution, then (4.16) gives an infinity of further solutions. We find that there are no solutions for  $\eta = 1, 2$  or  $5$ ; for  $\eta = 4$  there is the unique solution  $\phi = 51, \theta = 26$  which leads to the  $K_3N$   $43 \cdot 451 \cdot 607 = 11771551$  with  $B = 75$ ; while for each  $\eta \in \{3, 6, 7\}$  there are four fundamental solutions from which all other solutions can be derived via (4.16), but the only admissible ones are  $\phi = 14, \theta = 9$  for  $\eta = 3$  and  $\phi = 90, \theta = 35$  for  $\eta = 7$ , for which  $\phi^2 - 7\theta^2 = -475$  reduces to  $X^2 - 7Y^2 = -19$  via  $\phi = 5X, \theta = 5Y$ .

With reference to (4.16), amended as above, we need to show that for  $\eta \leq 7$  any solution  $(\phi_i, \theta_i)$  is admissible iff its fundamental solution  $(\phi_1, \theta_1)$  is admissible. From (4.16)  $\theta_{i+1} \equiv \theta_i \pmod{2}$ , so  $(\theta_{i+1} - \eta)$  is even iff  $(\theta_i - \eta)$  is even. Also the inverse transformation for (4.16) has  $\phi_i = (2\eta y^2 + 1)\phi_{i+1} - 2\eta xy\theta_{i+1}$ , and we have  $\eta y^2 = (x-1)(x+1)$ , so if  $xy$  is odd then  $8 \mid \eta$ , whence  $xy$  is even for  $\eta \leq 7$ . Working now in  $\mathbb{Z}_{4\eta}$  with  $\eta \leq 7$ , if  $y$  is even then  $\phi_{i+1} = \phi_i$ , and if  $\eta$  is even then  $x$  is odd and  $y$  is even. But if odd  $\eta = 2\nu + 1$  and  $y$  is odd, suppose  $\phi_i = \eta - 1$ ; then  $\phi_{i+1} = (2\eta y^2 + 1)\phi_i = (2\eta + 1)(\eta - 1) = 2\nu(2\eta + 1) = 4\nu\eta + \eta - 1 = \eta - 1$ ; conversely by the inverse transformation  $\phi_i = (2\eta y^2 + 1)\phi_{i+1}$ , so  $\phi_{i+1} = \eta - 1$  iff  $\phi_i = \eta - 1$ , whence by induction  $\phi_i = \eta - 1$  iff  $\phi_1 = \eta - 1$ . Thus as required  $(\phi_i, \theta_i)$  is admissible iff  $(\phi_1, \theta_1)$  is admissible. Also for acceptability we require  $E \geq 2$ : it is easily shown that  $E = F = G = 1$  gives rise to  $\eta = H^4 + 2H^3 + H^2 + H + 1$  (cf (4.18) and Theorem 4.4), so  $\eta = 39$  (with  $H = 2$ ) is the least  $\eta$  with an admissible solution with  $E = 1$ ; thus  $E \geq 2$  for  $\eta \leq 7$ .

With  $\eta = 3$ , the solution  $\phi = 14, \theta = 9$  gives the  $C_3N$   $7 \cdot 23 \cdot 41 = 6601$ , but this is the only  $C_3N$ , since we find in  $\mathbb{Z}_7$  that the cycles given by (4.16) are of period 4, and in  $\mathbb{Z}$  with obvious notation  $\gcd(A_{4i+2}, B_{4i+2}, C_{4i+2}) = 7$ , not acceptable, and  $p_{4i+1} \equiv p_{4i+3} \equiv q_{4i} \equiv r_{4i} \equiv 0 \pmod{7}$ . This is sufficient for our proof, but for  $\eta = 7$  the solution  $\phi = 90, \theta = 35$  gives the  $C_3N$   $43 \cdot 433 \cdot 643 = 11972017$  with  $B = 72$ , and there seems to be the *possibility* of further  $C_3N$ 's in the sequence of  $K_3N$ 's generated by (4.16).

It remains to show that for  $\eta = 3$  or  $7$  and any even  $H \geq 2$ ,  $B(H, \eta) < B_\eta(n(H, \eta))$ . If we write (4.26) as  $B = 2H^2 + 2H + \frac{4+\eta}{2} - \sqrt{\eta}H(1+x(H, \eta))^{\frac{1}{2}}$  and (4.27) as  $\frac{n}{4} = H^8(1+y(H, \eta))$ , then for large  $H$  with  $x := x(H, \eta)$  and  $y := y(H, \eta)$  we have  $x = O(\frac{1}{H})$ ,  $y = O(\frac{1}{H})$  and  $B_\eta(n) = 2H^2(1+y)^{\frac{1}{4}} - H(\sqrt{\eta} - \frac{1}{2})(1+y)^{\frac{1}{8}} + \frac{3\eta+4}{8} - \frac{\eta-4}{8\sqrt{\eta}}$ . Using the binomial series and omitting the complicated details we get

$$B_\eta(n) - B = \left( \frac{3\eta\sqrt{\eta}}{32} - \frac{\eta}{64} + \frac{15\sqrt{\eta}}{128} + \frac{117}{256} - \frac{1}{4\sqrt{\eta}} - \frac{1}{8\eta\sqrt{\eta}} \right) \frac{1}{H} + O\left(\frac{1}{H^2}\right) > 0$$

for sufficiently large  $H$ . To prove the result rigorously for all even  $H = H_o$ , we can truncate the various binomial series and approximate  $x$  and  $y$  to form functions  $b_\eta(n(\eta, H)) = b_\eta(n)$  and  $b(\eta, H) = b$  such that  $B_\eta(n) > b_\eta(n)$  and  $b > B$ , with  $b_\eta(n)$  and  $b$  containing a relatively small number of terms all of which are retained, whence for each  $\eta$  we can determine a precise  $H^*(\eta)$  such that  $b_\eta(n) - b > 0$  for  $H \geq H^*(\eta)$ . My method of truncation and approximation was as arithmetically economical as I could make it, subject to retaining exactly the above term in  $\frac{1}{H}$ , and after heavy detail arrived at  $H^*(3) = 240$  and  $H^*(7) = 66$ ; Gordon Davies (see §5.1) did the computer verifications for  $2 \leq H \leq H^*(\eta)$ .



Thus for any  $K_3N$  with  $F_o = G_o = 1$ , we have  $\eta_o \geq 3$  and for any  $C_3N$  except 6601 we have  $\eta_o \geq 7$ , so with  $\eta_a = 3$  or 7 as appropriate we have  $\eta_o \geq \eta_a$  and  $B_o = B(H_o, \eta_o) \leq B(H_o, \eta_a) < B_{\eta_a}(n(H_o, \eta_a)) \leq B_{\eta_a}(n(H_o, \eta_o)) = B_{\eta_a}(n_o)$  as required.  $\square$

We can construct a  $K_3$ -family  $\{n_4(t)\}$  such that, for any fixed  $\mu \geq 1$  and large  $t$ ,  $B(t) \sim B_\mu(n_4(t)) \sim B_{\eta(t)}(n_4(t)) \sim \sqrt{2} \sqrt[4]{n_4(t)}$  as follows:  $F = G = 1$  and then  $H = t(t+1)$ ,  $A = \eta = t^2 + t + 1$ ,  $s = tA$ , giving  $p_4(t) = t^4 + 2t^3 + 2t^2 + t + 1$ ,  $B(t) = 2t^4 + 3t^3 + 3t^2 + t + 2$ ,  $C(t) = 2t^4 + 5t^3 + 6t^2 + 4t + 3$ ,  $q_4(t) = 2t^6 + 5t^5 + 6t^4 + 4t^3 + 3t^2 + 2t + 1$ ,  $r_4(t) = 2t^6 + 7t^5 + 11t^4 + 10t^3 + 7t^2 + 3t + 1$  and  $n_4(t) = p_4(t) \cdot q_4(t) \cdot r_4(t)$ . Then we have  $B \sim 2t^4$  and  $n \sim 4t^{16}$ , so  $B \sim \sqrt{2} \sqrt[4]{n} \sim B_\mu(n) \sim B_\eta(n)$ . Then  $n_4(1) = 6601$  and  $n_4(2) = 11972017$  as above, but we found no more  $C_3N$ 's up to  $t = 31$ . Obviously (4.29) is satisfied identically by the parametric forms for  $H$ ,  $\eta$  and  $s$  of  $\{n_4(t)\}$ , since  $F = G = 1$ .

For  $\eta = 7$  and  $(\phi_1, \theta_1) = (90, 35)$ , (4.16) gives  $(\phi_2, \theta_2) = (23190, 8765)$  which yields the  $K_3N$   $n = 2743993 \cdot 9080853193 \cdot 9095368033$  with  $B = 5483607$ ,  $H = 1656$  and  $B_7(n) = 5483607.001$  (calculator accuracy).

We note that for the sequence of  $K_3N$ 's associated with Theorem 4.3 and (4.16) for given  $F \geq 3$ ,  $B \sim \sqrt{2} \sqrt[4]{\frac{n}{F}}$ . I confidently conjecture from the above proof of Theorem 4.8 and from numerical evidence that  $B < B_\eta(n)$  for every  $K_3N$ , but have not attempted a general proof.

Challenge 4: Find a  $C_3N$  for which  $n > 6601$  and  $B_7(n) - B < 0.1$ .

To conclude §4 we shall show that the  $K_3$ -families deriving from (4.18) and (4.19), with  $E = 2$  and  $F = G = 1$ , not only give equality for the upper bound for  $C$  given  $p$ , as described in the discussion following Theorem 4.4, but in the same way give equality for upper bounds for  $C, BC, ABC$  and  $n$  given  $H$ , and for  $C$  and  $ABC$  given  $n$ . Using the notation of (4.18) and (4.19):

**Theorem 4.9.** *For any  $K_3N$ , (a)  $C \leq C(H)$ , (b)  $BC \leq B(H) \cdot C(H)$ , (c)  $ABC \leq A(H) \cdot B(H) \cdot C(H)$  and (d)  $n \leq N(H)$ , with equality iff  $E = 2$  and  $F = G = 1$ . If there is equality then  $H \not\equiv 2 \pmod{6}$ , and if also  $n$  is a  $C_3N$ , then  $H \equiv 0 \pmod{6}$ .*

*Proof.* From (2.18),  $A = \frac{H+G}{F}$ , and then via (2.19), (2.16) and (2.6) we can express  $B, C, n$  (and obviously also  $p, q, r$ ) in terms of  $E, F, G, H$ . We now regard all other variables as functions of continuous real variables  $E, F, G, H$ , subject to all the relations so far established for  $K_3N$ 's. Let  $Z$  be any of, or any product from,  $A, B, C$  and  $n'$ : regarding  $H$  as fixed, we write  $\phi_Z(E, F, G) := Z$  evaluated at  $(E, F, G)$ . From (2.6) and (2.18) we have  $n' = ABC H^3 + BCH(G+H)$ , and then we readily see that  $F$  occurs only in the denominator of any  $Z$ , and thence

$$(4.30) \quad \phi_Z(E, F, G) < \phi_Z(E, 1, G) \quad \text{unless} \quad F = 1$$

**Lemma 4B.** *If  $f(x) := ax + \frac{b}{x}$  with  $a > 0, b > 0$ , then for  $0 < x_1 < \sqrt{\frac{b}{a}}$  we have  $f(x_1) > f(x)$  iff  $x_1 < x < \frac{b}{ax_1}$ .*

This follows at once from

$$f(x_1) - f(x) = a(x_1 - x) + b\left(\frac{1}{x_1} - \frac{1}{x}\right) = (x - x_1)\left(\frac{b}{xx_1} - a\right)$$

From (2.16, 2.18, 2.19) we have

$$(4.31a) \quad C = \frac{ABH + A + B}{E} = \frac{1}{E} \left\{ \left( \frac{H+G}{F} \right) \left( \frac{H^2+GH}{FG} + \frac{E+1}{G} \right) H + \frac{H+G}{F} + \left( \frac{H^2+GH}{FG} + \frac{E+1}{G} \right) \right\}, \quad \text{i.e.}$$

$$(4.31b) \quad C = \phi_C(E, F, G) = \frac{1}{EF^2} \left\{ (H^2 + F)G + \frac{H^2(H^2 + 2F)}{G} \right\} + \frac{2H^3}{EF^2} + \frac{H}{F} + \frac{3H}{EF} + \frac{1}{G} + \frac{1}{EG} + \frac{H^2}{FG}$$

Obviously since  $E \geq 2$ ,

$$(4.32) \quad \phi_C(E, F, G) < \phi_C(2, F, G) \quad \text{unless} \quad E = 2$$

Similarly, the last three terms of (4.31b) increase as  $G$  decreases. Also, applying Lemma 4B with  $x = G$ ,  $f(G) := (H^2 + F)G + \frac{H^2(H^2 + 2F)}{G}$  and  $x_1 = 1$  since  $G \geq 1$ , we have  $f(1) > f(G)$  iff  $1 < G < \frac{H^2(H^2 + 2F)}{H^2 + F}$ . But from Theorem 2.3,  $G < 2H$ , and since  $H \geq 2$  we have  $1 \leq G < 2H \leq H^2 < H^2(\frac{H^2 + 2F}{H^2 + F})$ , so  $f(1) > f(G)$  unless  $G = 1$ . Hence from (4.31b),

$$(4.33) \quad \phi_C(E, F, G) < \phi_C(E, F, 1) \quad \text{unless} \quad G = 1$$

Applying (4.30, 4.32, 4.33) in turn,

$$(4.34) \quad C = \phi_C(E, F, G) < \phi_C(2, 1, 1) \quad \text{unless} \quad E = 2 \text{ and } F = G = 1$$

Combining this with the discussion of (4.18) and (4.19), we have Theorem 4.9(a).

Also  $B = \frac{H}{F} + \frac{H^2}{FG} + \frac{E+1}{G}$  (as in (4.31a)), so  $\phi_B(E, F, G) < \phi_B(E, F, 1)$  unless  $G = 1$ , and hence with (4.33)

$$(4.35) \quad BC = \phi_{BC}(E, F, G) < \phi_{BC}(E, F, 1) \quad \text{unless} \quad G = 1$$

Now given  $F, G$  and  $H$ , also determined are  $A = \frac{H+G}{F}$  and  $p = AH + 1$ . Hence from (2.19) and (2.16) we have

$$\begin{aligned} \phi_{BC}(E, F, G) &= \left( \frac{p+E}{G} \right) \left( \frac{Bp+A}{E} \right) = \frac{p+E}{G} \left( \frac{p^2 + pE + AG}{EG} \right) \\ &= \frac{p}{G^2} \left\{ E + \frac{p^2 + AG}{E} \right\} + \frac{2p^2 + AG}{G^2} \end{aligned}$$

Applying Lemma 4B with  $x = E$ ,  $f(E) = E + \frac{p^2 + AG}{E}$  and  $x_1 = 2$  since  $E \geq 2$ , we have  $f(2) > f(E)$  iff  $2 < E < \frac{p^2 + AG}{2}$ , which is true unless  $E = 2$ , since  $p \geq 3$  and by Theorem 2.2,  $E \leq p - 1$ . Thus

$$(4.36) \quad \phi_{BC}(E, F, G) < \phi_{BC}(2, F, G) \quad \text{unless} \quad E = 2$$

Hence from (4.30, 4.35, 4.36),

$$(4.37) \quad BC = \phi_{BC}(E, F, G) < \phi_{BC}(2, 1, 1) \quad \text{unless} \quad E = 2 \text{ and } F = G = 1,$$

and Theorem 4.9(b) follows as for 4.9(a).

Also  $A$  is independent of  $E$ , so from (4.36)

$$(4.38) \quad \phi_{ABC}(E, F, G) < \phi_{ABC}(2, F, G) \quad \text{unless} \quad E = 2$$

$$\begin{aligned} \text{Further, } AB = \phi_{AB}(E, F, G) &= \frac{H+G}{F} \left( \frac{H^2 + GH + F(E+1)}{FG} \right) \\ &= \frac{H}{F^2} \left( G + \frac{H^2 + F(E+1)}{G} \right) + \frac{2H^2 + F(E+1)}{F^2}, \end{aligned}$$

so applying Lemma 4B with  $x = G$ ,  $f(G) = G + \frac{H^2 + F(E+1)}{G}$  and  $x_1 = 1$  since  $G \geq 1$ , we have  $f(1) > f(G)$  iff  $1 < G < H^2 + F(E+1)$ , which is true unless  $G = 1$ , since  $H \geq 2$  and from Theorem 2.3,  $G < 2H$ . Hence

$$(4.39) \quad \phi_{AB}(E, F, G) < \phi_{AB}(E, F, 1) \quad \text{unless } G = 1.$$

Then from (4.33) and (4.39),

$$(4.40) \quad \phi_{ABC}(E, F, G) < \phi_{ABC}(E, F, 1) \quad \text{unless } G = 1,$$

and from (4.30, 4.38, 4.40)

$$(4.41) \quad ABC = \phi_{ABC}(E, F, G) < \phi_{ABC}(2, 1, 1) \quad \text{unless } E = 2 \text{ and } F = G = 1$$

and Theorem 4.9(c) follows as for 4.9(a).

Also from (4.38) and (4.40),  $\phi_{ABC}(E, F, G) < \phi_{ABC}(2, F, 1)$  unless  $E = 2, G = 1$  and from (2.6)  $n' = ABCH(H^2 + F)$ , so

$$\phi_{n'}(E, F, G) = \phi_{ABC}(E, F, G)H(H^2 + F) < \phi_{ABC}(2, F, 1)H(H^2 + F) = \phi_{n'}(2, F, 1)$$

unless  $E = 2, G = 1$ ; and from (4.30)  $\phi_{n'}(2, F, 1) < \phi_{n'}(2, 1, 1)$  unless  $F = 1$ . Thus  $n' = \phi_{n'}(E, F, G) < \phi_{n'}(2, 1, 1)$  unless  $E = 2$  and  $F = G = 1$ ; Theorem 4.9 follows as for 4.9(a).  $\square$

We now express our results for upper bounds for  $C$  and  $ABC$  given  $n$  in terms of the functions of (4.18) and the inverse function  $N^{-1}$  of (4.19); using the method of Theorem 3.5, we could also express our results as series of descending powers of  $\sqrt[10]{n}$ , but we simply indicate the leading terms:

**Theorem 4.10.** *For any  $K_3N$ , (a)  $C \leq C(N^{-1}(n))$  and (b)  $ABC \leq A(N^{-1}(n)) \cdot B(N^{-1}(n)) \cdot C(N^{-1}(n))$  with equality as in Theorem 4.9. For large  $n$ ,  $C \leq 2^{-\frac{2}{5}}n^{\frac{2}{5}}(1 + o(1))$ ,  $ABC \leq 2^{-\frac{3}{10}}n^{\frac{7}{10}}(1 + o(1))$ .*

*Proof.* Suppose that all variables are real as in the proof of Theorem 4.9, and that  $(E, F, G) = (2, 1, 1)$ ; then  $n = N(H)$ ,  $H = N^{-1}(n)$ , so  $A = A(N^{-1}(n))$ , etc. Also the first part of the proof of Theorem 3.6 applies, with  $i = d = 3$  and  $\lambda_d = E = 2$ , giving  $r = \frac{\sqrt{8n+1}+1}{4}$ . But  $C = \frac{r'}{H}$ , so we have the functional relationship

$$(4.42) \quad C(N^{-1}(n)) = \frac{\sqrt{8n+1}-3}{4N^{-1}(n)}$$

Similarly from (2.6) we get

$$(4.43) \quad A(N^{-1}(n)) \cdot B(N^{-1}(n)) \cdot C(N^{-1}(n)) = \frac{n'}{N^{-1}(n)\{(N^{-1}(n))^2 + 1\}}$$

Now suppose that  $n$  is any  $K_3N$  with its standard  $A$  to  $H$  integer set. Then (a)  $C = \frac{r'}{H}$ , from Theorem 3.7  $r' \leq \frac{\sqrt{8n+1}-3}{4}$  with equality iff  $E = 2$  and from Theorem 4.9  $H \geq N^{-1}(n)$  with equality iff  $(E, F, G) = (2, 1, 1)$ , and hence

$C \leq \frac{\sqrt{8n+1}-3}{4N^{-1}(n)} = C(N^{-1}(n))$  from (4.42), with equality iff  $(E, F, G) = (2, 1, 1)$ . Also (b) from (2.6)

$$ABC = \frac{n'}{H(H^2 + F)} \leq \frac{n'}{N^{-1}(n)\{(N^{-1}(n))^2 + 1\}} = A(N^{-1}(n)) \cdot B(N^{-1}(n)) \cdot C(N^{-1}(n))$$

from (4.43), with equality iff  $(E, F, G) = (2, 1, 1)$ . The first sentence of Theorem 4.10 follows.

Also for large  $n$  and equality, from (4.18) and (4.19) we have  $C \sim \frac{1}{2}H^4$ ,  $ABC \sim \frac{1}{2}H^7$  and  $n \sim \frac{1}{2}H^{10}$ , so  $H \sim (2n)^{\frac{1}{10}}$  and  $C \sim 2^{-\frac{3}{5}}n^{\frac{2}{5}}$ ,  $ABC \sim 2^{-\frac{3}{10}}n^{\frac{7}{10}}$ , giving the final part of Theorem 4.10.  $\square$

## 5. THE ALGORITHM AND ITS IMPLEMENTATION

**5.1. Acknowledgments.** This is the most convenient place to acknowledge my immense debt to my two friends who have carried out the computer implementation of my algorithms: firstly Gordon Davies, like me a retired teacher of mathematics at Haileybury College, England, who did the computing throughout the development stage, programming in BASIC V with 32-bit arithmetic, and by August 1999 taking us on his RISC-PC, running RISC OS 3.7 with 16 Mb of RAM, to  $C_3(2 \times 10^{18}) = 42720$  (where  $C_3(X)$  is the number of three-prime Carmichael numbers up to  $X$ ); and secondly Matthew Williams, a recent Haileybury student and Cambridge University computer science graduate, who then got us up to  $C_3(10^{24})$ , using his 1 GHz Athlon with 900 Mb of RAM and programming in C++ mostly with 64-bit arithmetic.

**5.2. Notation.** In this section we shall use the following upper bounds based on results in § 3 and § 4. Each of these could be replaced with a slightly greater and simpler bound with only marginal loss of efficiency. We seek all  $C_3N$ 's less than  $X$ , where for convenience  $X$  is not a  $C_3N$ , so  $n < X$ .

$$(a) p \leq p_M := \left\lceil \sqrt[3]{X} - \frac{4\sqrt{3}}{9}\sqrt[6]{X} \right\rceil \quad (\text{Theorem 4.6})$$

$$(b) A < A_M := \sqrt{3p'} - \frac{1}{2}\sqrt[4]{\frac{p'}{12}} \quad (\text{Theorem 4.2})$$

$$(c) B < B_M := 2p - \sqrt{p - \frac{3}{4}} + \frac{\sqrt{7} + 1}{2\sqrt{7}} \quad (\text{Theorem 4.3})$$

$$(d) q \leq Q_1 := P' \left( 2P - \sqrt{P - \frac{3}{4} + \frac{1}{2}} \right) + 1 \quad (\text{Theorem 3.1})$$

$$(e) q < Q_2 := \sqrt{\frac{X}{p}} - \sqrt{\frac{p}{12}} \quad (\text{Theorem 4.5})$$

$$(f) Z := \min(Q_1, Q_2)$$

$$(g) \text{ For any } CN \text{ } q \leq Q_3 := \left\lceil \sqrt[5]{2X^2} - \sqrt[10]{\frac{X^3}{64}} - \frac{1}{10}\sqrt[5]{\frac{X}{4}} + \frac{17}{20}\sqrt[10]{\frac{X}{4}} \right\rceil \quad (\text{Theorem 3.5})$$

**5.3. A brief description of four algorithms and the split range procedure.** In [12] Pinch describes the two algorithms which he used to find all  $CN$ 's up to  $10^{15}$ . We briefly describe these now, since we used them, slightly modified to take

advantage of  $d = 3$ , to do selective checks on our results for large  $X$ . In all these algorithms, for given  $X$  the outermost loop runs through all odd primes up to  $p_M$ .

In Pinch's first algorithm, which as modified by me for  $d = 3$  we call PI, for each  $p$ ,  $E$  runs through the range  $E_L(p, X) \leq E \leq p'$  (Theorem 2.2), where  $E_L(p, X)$  is a fairly complicated function, not given here, which I formulated using  $d = 3$  (so  $P = p < q$ ) to cut out some of the cases which would result in  $n > X$  (for  $p < \sqrt[4]{3X}$ ,  $E_L(p, X) = 2$ ); using  $E_L(p, X)$  reduced the time for PI by about a third. For each  $E$  a range of integer values of  $D$  is found, subject to  $1 \leq \Delta = DE - p^2 \leq 2p'$  (Theorem 2.3), and for each  $(E, D)$  pair  $q$  and  $r$  are calculated from (2.9).  $E$ , and  $D$  for each  $E$  descend through their ranges, and if  $r > \frac{X}{pq}$  next  $E$  is taken; else  $q, r$  and  $\lambda_1 = \frac{qr - 1}{p'}$  (§2.1) must be integers, with next  $D$  at the failure of any test, and  $q$  and  $r$  are tested for primality.

For large  $X$  the remaining algorithms are all significantly speeded up by the split-range procedure, which we briefly describe. Suppose that variables  $x$  and  $y$  are connected by the bilinear relation  $axy + bx + cy + d = 0$  with  $a > 0, \nabla := bc - ad > 0$ , and that  $x_1 > -\frac{c}{a}$ , so over the interval  $x_1 \leq x \leq x_2$ ,  $y$  decreases as  $x$  increases; and also that we wish to find integer pairs  $(x, y)$  over this interval, and that a trial where we start with  $x \in \mathbb{Z}$  (an  $x$ -trial) costs  $k$  times the cost of a  $y$ -trial. Then if  $\frac{dy}{dx} = -k$  at  $(\xi, \psi)$  we minimise the cost by using  $x$ -trials for  $x < \xi$  and  $y$ -trials for  $y < \psi$  (so  $x > \xi$ ). So if  $x_1 < \xi < x_2$  it pays to split the range at  $(\xi, \psi) = \left( \frac{\sqrt{\nabla} - \sqrt{kc}}{\sqrt{ka}}, \frac{\sqrt{k\nabla} - b}{a} \right)$  (as may easily be shown), with a saving, compared with using only  $x$ -trials and ignoring the cost of deciding whether to split, of approximately  $\frac{ka(x_2 - \xi)^2}{ax_2 + c}$   $y$ -trial costs.

Pinch's second algorithm as modified by me for  $d = 3$  (PII) for each  $p$  runs through all primes  $q$  satisfying  $p < q \leq Z$ . For each  $(p, q)$  pair it uses the Euclidean algorithm to find  $H$  and hence  $A = \frac{p'}{H}$ , and if  $A > A_M$  it takes next  $q$ . Else it finds  $L_1 := \frac{p'q'}{H} = \text{lcm}[p', q'], R = pq$ , and  $w$  such that  $wR \equiv 1 \pmod{L_1}$ , by the reverse Euclidean algorithm; then, since  $n = rR \equiv 1 \pmod{L_1}$ , we have  $r = w + uL_1$ , and also  $R' = Er'$  (2.1), so eliminating  $r$  we seek integer pairs  $(u, E)$  such that

$$(5.1) \quad L_1 Eu + w'E - R' = 0.$$

With  $u$  ascending and  $E$  descending we use the split range procedure, take next  $q$  when  $r > \frac{X}{pq}$ , and for each integer pair  $(u, E)$  we test  $r$  for primality.

Our first successful algorithm (HI, originally devised when seeking Perrin pseudo-primes, before we knew of other algorithms) is the same as PII as far as finding  $A < A_M$ . It then found  $r$  in essentially the same way as our main algorithm HII, described next.

HII was motivated by the realisation that as  $p$  becomes larger in HI many more pairs  $(p, q)$  will result in  $H$  small enough to give  $A > A_M$ ; and that by first analysing  $p' = AH$  such pairs need never be considered. Since  $H$  is even,  $A$  divides  $\frac{p'}{2}$  and,

taking the most favourable case as an example, if  $\frac{p'}{2}$  is prime (and so is a Sophie Germain prime) then  $A = 1, H = p'$  is the only possibility and all possible values of  $q$  will belong to the arithmetic progression (AP)  $q \equiv p \pmod{p'}$ , with  $q \leq Z$ . So for each  $p$  we factorise  $\frac{p'}{2}$  to find all possible pairs  $(A, H)$  with  $A < A_M$ , and we organise a set of AP's which will contain without repetition the resulting  $q$ -values, which we then test for primality. For each prime  $q$  we find  $B = \frac{q'}{H}$ ; we find integer pairs  $(C, F)$  from (2.5a), which is bilinear in  $C$  and  $F$ , determining the range of  $F$  as described below in § 5.4, and test  $r = CH + 1$  for primality.

**5.4. The implementation of the HII algorithm in more detail.** The basic idea of the HII algorithm is as stated above, and we now describe more fully a method of programming it, drawing attention to certain worthwhile economies (our own method was slightly more complicated, as we shall explain briefly in the next subsection). We structure our description in terms of several loops, beginning with the outermost as Loop 1. To find all  $C_3N$ 's with  $n < X$ , we begin by preparing a bitmap prime database up to at least  $Q_3$  and we calculate  $p_M$ .

**Loop 1:** for each  $p$  satisfying  $3 \leq p \leq p_M$ , we calculate  $A_M, B_M$  and  $Q_2$ , and form an array  $\{A(j)\}$  of possible  $A$  values. To do this we have  $A \mid \frac{p'}{2}$ , so suppose

that the prime factorisation is  $\frac{p'}{2} = \prod_{k=1}^{\mu} \rho_k^{\eta_k}$ , where  $\eta_k \geq 1$ . We have  $A(1) = 1$ , and for  $j \geq 2$  we can obtain  $A(j)$  by a process involving successive trial division of  $\frac{p'}{2}$  by ascending primes, for each new  $\rho_k$  multiplying all  $A(j)$  already found by  $\rho_k$  to form more possible  $A$  values (but taking care to avoid duplication when  $\eta_k \geq 2$ ), testing for  $A < A_M$  before adjoining  $A$  to the array, and storing the successive prime factors  $\{\rho\} := \{\rho_1, \rho_2, \dots, \rho_\delta\}$  of  $\{A(j)\}$  as they arise (so  $\delta \leq \mu$ ).

**Loop 2:** for each  $A(j) = A$ , we now develop a set of AP's which must contain  $q$  for any  $C_3N$  associated with  $(p, A)$ , with each AP having common difference  $p'$ , and we also obtain the corresponding set of AP's with common difference  $A$  which contains the associated  $B$  values. We denote the  $\lambda^{\text{th}}$  term of the  $i^{\text{th}}$  AP for  $q$  by  $q_\lambda(i)$ , so  $q_\lambda(i) = q_1(i) + \lambda'p'$ , and similarly for  $B_\lambda(i)$ . We have  $H = \frac{p'}{A}$ , and for use in Loop 3 we define  $F_o = \lfloor \frac{H}{A} \rfloor$  and  $\nu := (F_o + 1)A - H$ . Clearly  $B = \frac{q'}{H} < \frac{Q_2}{H}$  and  $B < B_M$ ; also in loop 3 we shall show that  $B < \frac{2p}{\nu}$ , so an upper bound for  $B$  is  $\beta := \min(B_M, \frac{Q_2}{H}, \frac{2p}{\nu})$ . Next we use the facts that  $q$  is prime and  $B$  is coprime to  $A$  to restrict the number of cases to be considered. For  $A > 1$  we use a sieving method with those  $\rho_k \in \{\rho\}$  which divide  $A$  to find  $\Phi(A) := \{t : 1 \leq t \leq A' \text{ and } \gcd[A, t] = 1\}$  and we define  $\Phi(1) := \{1\}$ . Then for each  $t$  we form  $B_1 = A + t$  and  $q_1 = B_1H + 1 = AH + tH + 1$ , and for  $A \geq 3$ , if  $H \not\equiv 0 \pmod{\rho_k} \exists t \in \Phi(A)$  such that  $t \equiv -\frac{1}{H} \pmod{\rho_k}$  and then  $q_1 \equiv 0 \pmod{\rho_k}$ , so  $q_\lambda = q_1 + \lambda'p' = q_1 + \lambda'AH \equiv 0 \pmod{\rho_k}$  and thus the AP  $\{q_\lambda\}$  is entirely composite. Therefore if  $\rho_k \mid q_1$  we do not adjoin  $B_1$  or  $q_1$  to the arrays  $\{B_1(i)\}$  or  $\{q_1(i)\}$  (Gordon found that up to  $X = 10^{18}$  this eliminated from consideration about 19% of the potential AP's). So we form the arrays  $\{B_1(i)\}$  and  $\{q_1(i)\}$  of first terms and we use the iterations  $B_\lambda(i) = B_{\lambda-1}(i) + A$  and  $q_\lambda(i) = q_{\lambda-1}(i) + p'$  to form arrays  $\{B_\lambda(i)\}$  and  $\{q_\lambda(i)\}$ , having first examined each  $B_{\lambda-1}(i)$  for associated  $C_3N$ 's as described in Loop 3

below. Having used a sieving method to find  $\Phi(A)$ , we get  $B_\lambda(i)$  and  $q_\lambda(i)$  increasing steadily throughout this process, and  $B_\lambda(i) > \beta$  triggers next  $A(j)$ .

**Loop 3:** We write  $B_{\lambda-1}(i) = B$  and  $q_{\lambda-1}(i) = q$ , and if  $q$  is composite (check against bitmap prime database), we take next  $B$  and  $q$ . Writing  $K := AB, U := KH + A + B = Bp + A$  and  $V := (A + B)H + 1 = p + q'$ , (2.5a) may be written

$$(5.2) \quad KCF - VC - U = 0$$

and we use this bilinear relation in  $C$  and  $F$  to find integer pairs  $(C, F)$  and hence possible  $r = CH + 1$ . Theorems 2.1 and 4.4 suggest that we consider the  $F$ -range, and we examine certain related economies including a procedure for splitting the range.

Put  $Y := \frac{X}{pq} - 1$  and  $T := B + 1$ . Then  $r = \frac{n}{pq} < \frac{X}{pq}$ , so  $r' = CH < Y$ , and using (5.2) we get  $F > f_L := \frac{HU + YV}{KY}$ ; and  $C \geq T$  whence  $F \leq f_M := \frac{U + TV}{KT}$ . So if  $F_L := \lceil f_L \rceil$  and  $F_M := \lfloor f_M \rfloor$ , we need integer pairs  $(C, F)$  such that  $F_L \leq F \leq F_M$ . We easily show that

$$f_L(B) := f_L = \frac{H}{A} + \frac{p}{AB} + \frac{pH(Bp + A)(HB + 1)}{AB(X - p - pH B)}$$

$$\text{and } f_M(B) := f_M = \frac{H}{A} + \frac{p}{A} \left( \frac{1}{B} + \frac{1}{B + 1} \right) + \frac{1}{B(B + 1)}$$

Clearly  $f_L < f_M$ , but we can get  $F_M = \lfloor f_M \rfloor < f_L < f_M < \lceil f_L \rceil = F_L$ , in which case there are no possible  $F$  values. Further, as  $B \uparrow$ , both  $f_L(B) \downarrow$  and  $f_M(B) \downarrow$ , and also  $F_o = \lfloor \frac{H}{A} \rfloor \leq \frac{H}{A} < f_L \leq F_L$ , so if  $F_M = F_o$ , then we take next  $A(j)$  (at  $X = 10^{18}$  Matthew found that this  $F_M = F_o$  trigger reduced the program time by 20%). It is easily shown that

$$f_M\left(\frac{2p}{\nu} - 1\right) = F_o + 1 + \frac{\nu^2(p + A)}{2Ap(2p - \nu)} > F_o + 1 > F_o + 1 - \frac{\nu^2(p - A)}{2Ap(2p + \nu)} = f_M\left(\frac{2p}{\nu}\right)$$

whence  $F_M(\frac{2p}{\nu}) := \lfloor f_M(\frac{2p}{\nu}) \rfloor = F_o$ , justifying  $B < \frac{2p}{\nu}$ , anticipated in Loop 2.

A further though smaller economy can be achieved by eliminating from consideration some or all of those  $B$  values for which  $F_o + 1 < f_L < f_M < F_o + 2$  and so  $F_L > F_M$ : if then  $f_L(\beta) > F_o + 1$ , we can take next  $A$ ; if not, it can be shown that if  $\alpha := \sqrt{\nu^2 - \frac{4p^3H^2}{X}}$  then  $f_L(\frac{2p}{\nu + \alpha}) \simeq F_o + 1$ , so we can jump to  $B \simeq \frac{2p}{\nu + \alpha}$  to find  $f_L(B)$  just greater than  $F_o + 1$  and then continue (but this is awkward to program).

We next consider splitting the range (see §5.3) and a method of economising on  $C$ -trials which arranges them in an AP, first term  $C_o$ , say, and common difference  $e \in \{1, 2, 3, 6\}$ . Consider the conditions (a)  $2 \mid AB$  and (b)  $3 \mid AB$  and  $3 \nmid H$ . If only (a) holds,  $C$  is odd and  $e = 2$ . If only (b) holds, for  $C \equiv -\frac{1}{H} \pmod{3}$  we have  $r = CH + 1 \equiv 0 \pmod{3}$ , so  $C \not\equiv 0 \pmod{3}$  and  $C \not\equiv -\frac{1}{H} \pmod{3}$ , leaving only one possible residue, and  $e = 3$ . If both (a) and (b) hold, then  $e = 6$ , and if neither,  $e = 1$ . Then by eliminating as appropriate for each situation over the range  $B + 1 \leq C \leq B + e$  if  $2 \mid C$ ,  $3 \mid C$  or  $3 \mid r$ , we find  $C_o$ . With the notation of §5.3 and with  $x = C$ , it seems reasonable to take  $k = \frac{1}{e}$  and then  $\xi = \sqrt{\frac{eU}{K}} \simeq \sqrt{eH}$ .

So to execute the loop, as described above, we see whether  $F_M$  and  $F_L$  values permit us to take next  $A$  (or possibly to jump some  $B$ 's); and then if  $F_L > F_M$  we take next  $B$ . If  $B < \sqrt{eH}$  we do  $C$ -trials until  $C \geq \sqrt{eH}$ , taking next  $B$  if  $F < F_L$  while  $C < \sqrt{eH}$ , and then  $F$ -trials; but if  $B \geq \sqrt{eH}$  we do

$F$ -trials for  $F_L \leq F \leq F_M$ . For  $C$ -trials  $F = \frac{F_T}{F_B}$  where  $F_T := U + VC$  and  $F_B := KC$ , so with  $V^* = eV$  and  $K^* = eK$  we start with  $C = C_o$  and then do  $F_T \rightarrow F_T + V^*$  and  $F_B \rightarrow F_B + K^*$  to find  $F$  for next  $C$ ; and similarly for  $F$ -trials with  $C = \frac{U}{KF-V} = \frac{U}{E}$  we do  $E \rightarrow E + K$  for unit increase in  $F$ . Also if  $F_L$  gives  $E = 1$ , we take next  $E$ .

Each  $(C, F)$  integer pair then gives  $r = CH + 1$  which we test for primality, using the standard algorithm if  $r$  is beyond the bitmap prime data base.

**5.5. Some notes on our implementation of HII.** (i) In the development stage, to test  $q$  for primality we used a carefully designed but complicated system of tracking through a prime database, exploiting the advance of the arrays  $\{q_\lambda(i)\}$  by  $p'$  for each unit increment in  $\lambda$ , and we also had much less RAM. For these reasons we constructed arrays  $\{q_\lambda(i)\}$  for each  $p$ , rather than each  $A$ , which involved extra complications with certain loop exits. But then Matthew found that primality testing for  $q$  was taking at least 80% of the time, and constructed the bitmap database, which at  $X = 10^{18}$ , for example, reduced the program running time by a factor of at least 5, and was a major contribution to what we were able to achieve. Nevertheless we did not revise the array structure, as we estimated this would have given only a marginal decrease in time.

(ii) In §5.7 we shall give some running times, so we mention that the Loop 3  $F_M = F_o$  trigger was a late discovery, and right up to  $C_3(10^{24})$  our implementation only used the special case  $F_M = 0$ , which Matthew's later trial showed gives about 60% of the 20% time saving available at  $X = 10^{18}$ .

**5.6. A faster algorithm?** If  $(C^*, F^*)$  is an integer pair, it follows from the theory of PII outlined in § 5.3 (or directly from (5.2)) that a necessary condition for  $(C, F)$  to be an integer pair is  $C = C^* + Ku$ , and then (5.1) and (5.2) give

$$(5.3) \quad KuF + C^*F - Vu - C^*F^* = 0,$$

an even more discriminating bilinear relation, between  $F$  and  $u$ . The total number of trials when the split range is used with (5.2) is approximately  $2\sqrt{H} - T - \frac{H^2}{Y}$ , so when this is very large (big  $H$ , very big  $X$ ), using (5.3) might be worth the cost of finding  $(C^*, F^*)$  — either by the method of PII for  $w$ , or simply using (5.2) until (and if) such a  $(C^*, F^*)$  is encountered. We did not implement this.

**5.7. Comparison of algorithms for  $d = 3$ .** Ignoring time required for primality testing of  $q$  in PI and HII (by virtue of “bitmap”) and of  $r$  (relatively seldom required and the same for all four programs), and based on the number of test pairs  $(E, D), (p, q), (C, F)$  involved, I deduced that PI, PII and HI are all  $O(X^{\frac{2}{3}+o(1)})$ ; in the range  $10^{12} \leq X \leq 10^{16}$  for all three programs when  $X$  was multiplied by 10 the multiplier for the time was close to 4.325 and slowly increasing with  $X$ , giving some support to this deduction since  $10^{\frac{2}{3}} \simeq 4.64$ . On the same basis I conjecture but have not succeeded in establishing that HII is  $O(X^{\frac{1}{2}+o(1)})$ , and over the range  $10^{16} \leq X \leq 10^{18}$  the corresponding time multiplier was 3.013, slightly less than  $10^{\frac{1}{2}} \simeq 3.162$ .

Here are a few of the many times recorded. Illustrating the effects of improvements in computer technology, more powerful algorithms and the use of a compiled in place of an interpreted language, Gordon first reached  $C_3(10^{12}) = 1000$  early in 1998 with an early version of HI on a mid-1980's computer in about 45 hours; in



November 2001 it took Matthew 0.19 seconds actual calculating “user” time (1.15 seconds total). Gordon on his new computer (see §5.1), with HII and my  $q$  primality testing method (see subsection 5.5(i)) in mid 1999 took about 32 seconds for  $C_3(10^{12})$  and  $35\frac{1}{2}$  hours for  $C_3(10^{18})$ ; in mid 2000  $C_3(10^{18})$  took Matthew  $10\frac{3}{4}$  minutes with a slightly improved prime testing method and compiler optimisation, and finally with this method fully replaced by bitmap it took just 2 minutes 7.59 seconds. In July 2002  $C_3(10^{24})$  took about 58 hours, with about 9 minutes for the bitmap.

RAM and time constraints prevented us from going on to  $X = 10^{25}$ .

**5.8. Checking and correction.** Up to  $X = 10^{18}$ , Gordon and I had Richard Pinch’s paper [12] and his Internet results to check against. We achieved agreement up to  $10^{17}$ , but at  $10^{18}$  we found that his list omitted  $n^\dagger = 835327 \cdot 893359 \cdot 1117117 = 833645090806507981$  (for more on  $n^\dagger$ , see discussion following Theorem 4.1). Richard told me that  $n^\dagger$  inexplicably failed to reach the Internet list, although his program gave it. He also kindly put me in touch with Carl Pomerance, who sent me the first preprint of [10] and invited Gordon Davies and me to attempt the awkward evaluation of the constant  $\kappa_3$  (see [6]). Some months later when Carl asked us for any counts we had beyond  $X = 10^{18}$ , Matthew had got to  $X = 10^{20}$ , but had not yet done any checks; it later emerged that a problem in the program was by  $X = 10^{20}$  unfortunately causing omissions: the value of 120459 for  $C_3(10^{20})$  which we gave to Carl and is published in [10] should be 120625, and the number of imprimitive  $C_3N$ ’s up to  $10^{20}$  should be 89854.

Obviously comprehensive checking of HII results for large  $X$  with other known algorithms is not practicable. Soon after successfully programming PI, Matthew used it for a complete check at  $X = 10^{19}$ ; this took about  $62\frac{1}{2}$  hours, checking  $q$  for primality by the standard algorithm, and no discrepancy was found. For final checking he used PII to find the  $C_3N$ ’s corresponding to every  $k^{th}$   $p$ -value for  $X = 10^N$  for  $(N, k) = (19, 2), (20, 10), (21, 30), (22, 150), (23, 1000)$  and  $(24, 1000)$ , with initial  $p$  values chosen to cut down repetitions of the same check. No discrepancies were found. The last of these checking runs, at  $X = 10^{24}$ , took PII about 74 hours and HII about  $3\frac{1}{2}$  minutes.

We are grateful to Harvey Dubner for collaboration which gave a further partial check. Let  $C_3^\dagger(X) := \#\{n : n \text{ is a } C_3N \text{ with } A = 1, \text{ and } n \leq X\}$ . In [8] Dubner finds  $C_3^\dagger(10^N)$  up to  $N = 20$ , and suggests that for a “wide range of  $N$ ”,  $\frac{C_3^\dagger(10^N)}{C_3(10^N)} \simeq 0.644$ . He uses an entirely different algorithm for  $C_3^\dagger(X)$ , based on relevant  $(1, B, C)$  values. In correspondence he then took  $C_3^\dagger(10^N)$  up to  $N = 24$ , obtaining agreement with counts we have extracted from our discs for  $C_3(10^{23})$  and, later,  $C_3(10^{24})$ . In Table 1 of §6 we extend up to  $N = 24$  Dubner’s Table 2 for  $(1, B, C)$  in [8].

When finding  $C_3(X)$  for  $X \geq 10^{18}$ , we avoided the danger of rounding errors wrongly including or excluding a  $C_3N$  very close to  $X$  by doing a run to find  $C_3(X^*)$  with  $X^* = (1 + \epsilon)X$  and examining individually any  $C_3N$ ’s in the range  $(1 \pm \epsilon)X$ , where typically  $\epsilon = 10^{-3}$  or  $10^{-4}$  (at  $X = 10^{24}$  Matthew took  $\epsilon = 0.1$ ).

## 6. STATISTICS

In Table 1 we tabulate for  $X = 10^N$ , with  $3 \leq N \leq 24$ ,  $C_3(X)$  and various other numbers which we now define. In [10] Granville and Pomerance define *primitive*

$CN$ 's, and for  $C_3N$ 's their definition implies that a  $C_3N$  is primitive iff  $H \leq ABC$ ;  $C_3^*(X) := \#\{n : n \text{ is a primitive } C_3N \text{ and } n \leq X\}$ , and our data are consistent with their conjecture that  $\frac{C_3^*(X)}{C_3(X)} \rightarrow 0$  as  $X \rightarrow \infty$ .

Let  $\mathcal{C} := \{n : n = pqr \text{ is a } C_3N \text{ and } p \equiv q \equiv r \equiv -1 \pmod{4}\}$ ; Rabin showed in [15] that the probability of any odd composite  $n$  passing the strong pseudoprime test for a randomly chosen base  $b$  is less than  $\frac{1}{4}$ , and that this bound is approached most closely when  $n \in \mathcal{C}$ ; and Pinch lists various other properties of  $\mathcal{C}$  in [12];  $\mathcal{C}(X) := \#\{n : n \in \mathcal{C} \text{ and } n \leq X\}$

In § 8 of [10] Granville and Pomerance conjecture that  $C_3(X) \sim \tau_3 \frac{X^{\frac{1}{3}}}{(\log X)^3} \sim \frac{\tau_3}{27} \int_2^{X^{\frac{1}{3}}} \frac{dt}{(\log t)^3}$ , where  $\tau_3 \simeq 2100$  is a constant whose evaluation is discussed in [6];

they define  $\beta$  and  $\gamma$  by  $C_3(X) = \beta \frac{X^{\frac{1}{3}}}{(\log X)^3} = \frac{\gamma}{27} \int_2^{X^{\frac{1}{3}}} \frac{dt}{(\log t)^3}$  and predict that  $\beta$  and  $\gamma$  eventually converge to  $\tau_3$  from above and below respectively. Our new data are consistent with this, supporting their cautious comment in [10] (but see [6], Table 3 and comment).

$C_3^\dagger(X)$  is defined above in § 5.8.

TABLE 1.

$N$	$C_3(X)$	$C_3^*(X)$	$\frac{C_3^*(X)}{C_3(X)}$	$\mathcal{C}(X)$	$\beta$	$\gamma$	$C_3^\dagger(X)$	$\frac{C_3^\dagger(X)}{C_3(X)}$
3	1	1	1	0	32.96	9.092	1	1
4	7	7	1	1	253.9	53.13	6	0.8571
5	12	12	1	1	394.5	78.07	11	0.9167
6	23	19	0.826	1	606.5	128.1	18	0.7826
7	47	36	0.766	4	913.5	220.2	36	0.7660
8	84	59	0.702	8	1131	321.9	59	0.7024
9	172	113	0.657	15	1531	519.9	122	0.7093
10	335	208	0.621	29	1898	761.3	227	0.6776
11	590	338	0.573	50	2065	961.5	403	0.6831
12	1000	529	0.529	79	2110	1113	680	0.68
13	1858	930	0.501	153	2313	1349	1220	0.6566
14	3284	1550	0.472	271	2370	1496	2104	0.6407
15	6083	2621	0.431	487	2506	1680	3911	0.6429
16	10816	4201	0.388	868	2510	1763	6948	0.6424
17	19539	6814	0.349	1569	2525	1839	12599	0.6448
18	35586	11190	0.314	2837	2534	1899	22920	0.6441
19	65309	18432	0.282	5158	2538	1947	41997	0.6431
20	120625	30771	0.255	9443	2538	1984	77413	0.6418
21	224763	51432	0.229	17316	2541	2019	144300	0.6420
22	420658	85921	0.204	32351	2538	2047	270295	0.6426
23	790885	143620	0.182	61130	2531	2067	508780	0.6433
24	1494738	241562	0.162	115606	2523	2081	961392	0.6432

From Theorem 3.3 we have  $n \leq N_3(P) := \frac{1}{2}(P^6 + 2P^5 - P^4 - P^3 + 2P^2 - P)$ .

For any odd prime  $p$  we define  $\chi(p) := \#\{n : n \text{ is a } C_3N \text{ and } n = pqr\}$  and  $T(x) := \sum_{p \leq x} \chi(p)$ . Our list of  $C_3N$ 's up to  $10^{24}$  enables us to find  $\chi(p)$  and  $T(p)$  up to  $p = 11213$ , since we have  $N_3(11213) < 10^{24} < N_3(11239)$ . In Table 2 we tabulate  $p, \chi(p)$  and  $T(p)$  up to  $p = 211$ , and in Table 3  $p, T(p)$  for  $\pi(p)$  in intervals of 50 or 240 up to  $\pi(11213) = 1357$ .

$\chi(p) = 0$  for  $p = 11, 197, 1223, 1487, 4007, 4547, 7823, 9833, 9839$  and  $10259$ , and  $\chi(p) = 1$  for 51 values of  $p$ .  $\chi(211) = 17$  is the greatest value of  $\chi(p)$  until  $p = 1171$ ; with  $\chi(p) \geq 22$  we have  $\chi(p) = 22$  for  $p = 1171, 7481, 8521, 8647$  and  $10711$ ,  $\chi(9241) = 24$ ,  $\chi(10837) = 25$  and  $\chi(2221) = 29$ .

At first in Tables 2 and 3  $T(p)$  keeps remarkably close to  $p$  before going ahead for a bit, but then  $p$  gradually overhauls  $T(p)$  and seems to be slowly pulling away. Clearly  $C_3(X) \leq T(p_M)$ , and a plausible heuristic argument that  $T(p_M) \leq O(X^{\frac{1}{3}+o(1)})$  can be based on the loops of algorithm HII, ignoring the primality requirement on  $p, q, r$ . The best upper bound for  $C_3(X)$  which has so far been proved is  $O(X^{\frac{5}{14}+o(1)})$ , by Balasubramanian and Nagaraj in [1].

TABLE 2. Number and cumulative total of  $C_3N$ 's with first prime  $p$ 

$p$	3	5	7	11	13	17	19	23	29	31	37	41
$\chi(p)$	1	3	6	0	5	2	2	1	2	7	5	7
$T(p)$	1	4	10	10	15	17	19	20	22	29	34	41
$p$	43	47	53	59	61	67	71	73	79	83	89	97
$\chi(p)$	11	3	3	1	10	3	7	4	1	2	5	6
$T(p)$	52	55	58	59	69	72	79	83	84	86	91	97
$p$	101	103	107	109	113	127	131	137	139	149	151	157
$\chi(p)$	2	5	3	10	5	5	11	4	6	2	9	11
$T(p)$	99	104	107	117	122	127	138	142	148	150	159	170
$p$	163	167	173	179	181	191	193	197	199	211		
$\chi(p)$	7	2	3	4	11	6	10	0	7	17		
$T(p)$	177	179	182	186	197	203	213	213	220	237		

TABLE 3. Cumulative total in Table 2 extended

$\pi(p)$	47	97	147	197	247	297	347	397	637	877	1117	1357
$p$	211	509	853	1201	1567	1951	2341	2719	4723	6823	8999	11213
$T(p)$	237	565	896	1235	1556	1906	2299	2651	4347	6110	7945	9608

From (4.19) and Theorem 4.9(d) we have  $n \leq N(H) = \frac{1}{2}(H^{10} + 4H^9 + 14H^8 + 30H^7 + 53H^6 + 69H^5 + 71H^4 + 55H^3 + 31H^2 + 12H + 2)$ .

Since  $N(268) < 10^{24} < N(270)$ , we can in a similar way use our list of  $C_3N$ 's up to  $10^{24}$  to count all the  $C_3N$ 's for each  $H$  up to  $H = 268$ . Let  $\zeta(H) := \#\{n : n \text{ is a } C_3N \text{ with } \gcd[p', q'] = H\}$  and  $Z(x) := \sum_{H \leq x} \zeta(H)$ . We find  $\zeta(H) = 0$  for  $H = 68, 76, 160, 176, 188, 196$  and  $218$ ,  $\zeta(H) = 1$  for  $H = 98, 104, 134, 164, 184, 202, 212, 232, 244$  and  $248$ ; and the largest values are  $\zeta(210) = 19$ ,  $\zeta(H) = 18$  for  $H = 30, 60, 102$  and  $156$ ,  $\zeta(150) = 16$  and  $\zeta(198) = 13$ . Table 4 shows the growth of  $Z(H)$ .

TABLE 4. Cumulative total of  $C_3N$ 's with  $\gcd(p', q') \leq H$ 

$H$	20	40	60	80	100	120	140	160	180	200	220	240	260	268
$Z(H)$	44	98	162	204	263	334	390	450	491	531	578	646	687	705

Table 5 shows  $\#\{n : n \text{ is a } C_3N, n \equiv c \pmod{m} \text{ and } n \leq 10^N\}$  for various  $m, c$  and  $N$ .

TABLE 5. Cumulative totals of  $C_3N$ 's up to  $10^N$  satisfying  $n \equiv c \pmod{m}$ 

		N	7	9	11	13	15	17	19	21	23
m	c										
5	1		35	133	457	1405	4611	14716	49030	169157	595168
	2		1	6	40	133	455	1522	5151	17479	61711
	3		5	11	41	138	434	1421	4726	16108	56953
	4		3	19	49	179	580	1877	6399	22016	77050
7	1		22	102	339	1078	3472	11029	36668	125774	443797
	2		4	9	36	136	499	1660	5590	19280	68227
	3		4	18	54	171	501	1636	5645	19551	68150
	4		3	12	55	162	544	1766	6057	20990	73529
	5		4	10	46	133	494	1666	5379	18752	65616
	6		4	15	54	172	567	1776	5964	20410	71560
11	1		13	48	183	591	2063	6678	22417	77368	272654
	2		3	18	54	161	471	1499	4965	17230	60546
	3		2	13	43	134	432	1367	4729	16599	58510
	4		4	13	40	142	421	1362	4598	15971	55563
	5		4	13	47	151	435	1411	4756	16204	57647
	6		6	15	49	151	478	1515	4944	16670	58038
	7		2	10	34	127	443	1378	4711	16318	57489
	8		5	14	46	130	455	1511	4869	16543	57988
	9		4	12	48	115	420	1431	4748	16233	57508
	10		3	15	45	155	464	1386	4571	15626	54941
12	1		38	145	516	1632	5353	17221	57694	199002	700227
	5		4	11	23	72	242	748	2456	8444	29527
	7		4	15	50	153	478	1517	4994	16766	59215
	11		0	0	0	0	9	52	164	550	1915

In [12] Pinch describes and searches for certain special types of  $CN$  discussed by other authors, including *strong Fibonacci pseudoprimes* (of which he finds just one up to  $10^{18}$ , with  $d = 8$ ). These special  $CN$ 's all have the property that  $p_i + 1$  divides  $n \pm 1$  for  $1 \leq i \leq d$ , and for  $d = 3$  I have proved that no such numbers exist: see [14].

## 7. ACKNOWLEDGMENTS

I have already acknowledged the huge contributions of Gordon Davies and Matthew Williams. Their collaboration has been essential and most rewarding, and I am extremely grateful. As mentioned in § 5.3, HI was originally devised to

find  $C_3N$ 's which were also Perrin pseudoprimes in an earlier (unpublished) investigation and it was Gordon who originally suggested using it to pursue  $C_3(X)$ . I am also deeply indebted to my friend Ian Williams (Haileybury physics teacher and father of Matthew) for extracting from discs listing  $C_3N$ 's up to  $10^{23}$ , and then  $10^{24}$ , supplied by Matthew, the data for Tables 2, 3, 4, 5 and  $\mathcal{C}(X)$  and  $C_3^\dagger(X)$  in Table 1; for doing the  $K_3N$  or  $C_3N$  computer checks and searches required for and associated with Theorems 3.1, 3.3 and 4.8; and also for undertaking the massive task of converting my manuscript into  $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$ . I also thank Richard Pinch and Carl Pomerance for their encouragement and the stimulation of their work.

## REFERENCES

1. R.Balasubramanian and S.V.Nagaraj, *Density of Carmichael numbers with three prime factors*, Math. Comp. **66** (1997), 1705–1708
2. N.G.W.H.Beeger, *On composite numbers  $n$  for which  $a^{n-1} \equiv 1 \pmod{n}$  for every  $a$  prime to  $n$* , Scripta Mathematica **16** (1950), 133–135.
3. R.D.Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. (N.S.) **16** (1910), 232–238.
4. ———, *On composite numbers  $P$  which satisfy the Fermat congruence  $a^{P-1} \equiv 1 \pmod{P}$* , Amer. Math. Monthly **19** (1912), 22–27.
5. J.Chernick, *On Fermat's Simple Theorem*, Bull. Amer. Math. Soc. (N.S.) **45** (1939), 269–274.
6. J.M.Chick and G.H.Davies, *The evaluation of  $\kappa_3$* , Math. Comp. **77** (2008) 547–550.
7. Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, *PseudoPrimes*, <http://www.dpmms.cam.ac.uk/PseudoPrimes/Chick>
8. H.Dubner, *Carmichael Numbers of the form  $(6m+1)(12m+1)(18m+1)$* , (Internet) J. Integer Seq. **5**, Article 02.2.1
9. H.J.A.Duparc, *On Carmichael numbers*, Simon Stevin **29** (1952), 21–24.
10. A.Granville and C.Pomerance, *Two contradictory conjectures concerning Carmichael numbers*, Math. Comp. **71** (2001), 883–908
11. A.Korselt, *Problème chinois*, L'intermédiaire de mathématiciens **6**, (1899) 142–143
12. R.G.E.Pinch, *The Carmichael Numbers up to  $10^{15}$* , Math. Comp. **61** (1993), 381–391
13. ——— *The Carmichael Numbers up to  $10^{18}$* , arXiv:math/0604376v1 [math.NT] (17 April 2006)
14. *Problem Corner*, Mathematical Gazette **87** No. 507 (July 2003)
15. M.O.Rabin, *Probabilistic Algorithm for Testing Primality*, J. Number Theory **12** (1980), 128–138
16. P.Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag New York Inc, 1996
17. J.D.Swift, *Table of Carmichael numbers to  $10^9$* , Review 13, Math. Comp. **29** (1975), 338–339.

10 POSTWOOD GREEN, HERTFORD HEATH, HERTFORDSHIRE SG13 7QJ, UK